# Symantec™ Enterprise Firewall

## Installation Guide

### Supported platforms:

Microsoft Windows Server 2000

Microsoft Windows Advanced Server 2000

Microsoft Windows Server 2003 Standard Edition

Sun Solaris 8 (32 and 64-bit)

Sun Solaris 9 (64 bit)

# Symantec™ Enterprise Firewall Installation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 8.0

PN: 10202273

March 10, 2004

### Copyright notice

Copyright © 1998–2004 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

### Trademarks

Symantec, the Symantec logo, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. LiveUpdate, LiveUpdate Administration Utility, Symantec™ AntiVirus, and Symantec™ Security Response are trademarks of Symantec Corporation. RSA SecurID®, Bellcore S/KEY™, PassGo Defender™, Microsoft® Windows, Sun Solaris™, and Intel® Pentium®, are all the trademarks or registered trademarks of their respective companies.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

## Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works

collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

## Licensing and registration

This product requires a license file. The fastest and easiest way to register your service is to access the Symantec licensing and registration site at:

https://licensing.symantec.com

See "Licensing" on page 81.

## Contacting Technical Support

Customers with a current maintenance agreement may contact the Technical Support group by phone or online at:

www.symantec.com/techsupp/

Customers with Platinum support agreements may contact Platinum Technical Support by the Platinum Web site at:

www-secure.symantec.com/platinum/

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information

- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
- Error messages/log files
- Troubleshooting performed prior to contacting Symantec
- Recent software configuration changes and/or network changes

## Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com/techsupp/, select the appropriate Global Site for your country, then select the enterprise Continue link. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

# Contents


Chapter 1 Introducing the Symantec Enterprise Firewall

About Symantec Enterprise Firewall ..... 9
- Intended audience ..... 10
- Document structure ..... 10
- Developing a security plan ..... 11

Managing your client environment ..... 11
- Java Runtime Environment ..... 11
- Microsoft Windows hardware and software requirements ..... 12
- Sun Solaris hardware and software requirements ..... 14
- Supported network interface cards (NICs) in High Availability/Load Balancing mode ..... 15
- Understanding your installation options ..... 17

Where to get more information ..... 18

CD-ROM layout ..... 18
- For Microsoft Windows operating systems ..... 19
- For Sun Solaris operating systems ..... 19

Replacement CD-ROMs ..... 20

Chapter 2 Installing a security gateway on a Microsoft Windows server

Before you install ..... 21
- Configuring your Microsoft Windows operating system ..... 21
- Verifying your network configuration ..... 23
- Upgrading from Symantec Enterprise Firewall 7.x to Symantec Enterprise Firewall 8.0 ..... 25

Installing the Symantec Enterprise Firewall version 8.0 software ..... 26
- Installing RemoteLog ..... 27
- Using Vulture to disable unauthorized services ..... 27

Chapter 3 Installing the security gateway on a Sun Solaris 8 or 9 server

Before you install ..... 29
- Configuring your Solaris operating system ..... 29
- Verifying UNIX TCP/IP settings ..... 31

Upgrading from Symantec Enterprise Firewall 7.x to Symantec Enterprise Firewall 8.0 ..... 32
Installing the Symantec Enterprise Firewall version 8.0 software ..... 33
Installing RemoteLog ..... 34

Chapter 4 Using the System Setup Wizard

Understanding the System Setup Wizard ..... 37
Obtaining your license file ..... 38
Upgrading or restoring your configuration from Symantec Enterprise Firewall version 7.x ..... 38
Upgrading limitations ..... 39
Running the System Setup Wizard to restore a previous configuration ..... 40
Running the System Setup Wizard for initial configuration ..... 47
Configuring your security gateway ..... 55
Uninstalling the security gateway software ..... 55
Uninstalling the Microsoft Windows security gateway version 8.0 software ..... 55
Uninstalling the Sun Solaris security gateway 8.0 software ..... 56

Chapter 5 Verifying your installation

About verifying your installation ..... 59
Checking your basic network connectivity ..... 59
PING the security gateway by address ..... 60
PING an address on each inside network ..... 60
PING more than one subnet ..... 61
Checking your Internet connection ..... 61
Checking your network card ..... 62
Managing network interface cards ..... 62

Appendix A Developing a pre-installation security plan

About developing a security plan ..... 65
Defining your security policy ..... 65
Before writing your security plan ..... 66
Becoming security-conscious ..... 67
Educating users ..... 67
Involving the user community ..... 68
Filling out worksheets ..... 68
Defining your organization ..... 68
Collecting hardware information ..... 71
Collecting your TCP/IP address ..... 72
Defining your allowed TCP/IP services ..... 74
Collecting email information for security gateway notifications ..... 75

Defining your Web services ..... 76
Defining your network architecture ..... 78

Appendix B Licensing

Getting started with your 30-day grace period ..... 81
Easy steps for successful license implementation ..... 81
Gather your Serial Number Certificates ..... 82
Sort your serial numbers for each security gateway ..... 82
Collect product and contact information ..... 83
Plan for your license file ..... 84
Obtain your license file ..... 84
Understanding node count ..... 85
Example scenario of when one IP address acts as client and server ... 86
How licenses are counted for Client-to-Gateway VPN ..... 87
Understanding nodes within clusters ..... 87
Using the Symantec License Request & Maintenance Web site ..... 91
Getting your license files ..... 91
Uploading your license files ..... 96
Removing license files ..... 98
Viewing license enabled features ..... 98
Explanation of Symantec Enterprise Firewall licensing and maintenance ..... 100
Session licensing for Symantec Client VPN ..... 100
High Availability and Load Balancing (HA/LB) ..... 100
Obtaining a license file ..... 100
Basic license types ..... 100
Content updates ..... 102
Maintenance contracts ..... 102
Maintenance renewals ..... 103
Platinum support uplift ..... 103
About Symantec licenses ..... 103
SYMANTEC SOFTWARE LICENSE AGREEMENT
SYMANTEC ENTERPRISE FIREWALL ..... 103

Appendix C Troubleshooting

Accessing troubleshooting information ..... 107

Index

Chapter 1

# Introducing the Symantec Enterprise Firewall

This chapter includes the following topics:


- About Symantec Enterprise Firewall
- Managing your client environment
- Where to get more information
- CD-ROM layout
- Replacement CD-ROMs


## About Symantec Enterprise Firewall

This manual describes how to install Symantec Enterprise Firewall. Beginning with this release, the product is managed with the Security Gateway Management Interface (SGMI). The SGMI is a platform-independent, Java-based management system that replaces both the Symantec Raptor Management Console (SRMC) and the Raptor Console for UNIX (RCU). You access the SGMI through a standard Web browser over an encrypted channel pointed at the security gateway. This approach lets you manage a security gateway from the server itself or any client computer with a supported Web browser.

This manual describes installation for the following systems:

- Microsoft Windows Server 2000
- Microsoft Windows Advanced Server 2000
- Microsoft Windows Server 2003 Standard Edition

- Sun Solaris 8 (32 and 64 bit)
- Sun Solaris 9 (64 bit)

Consult the *Symantec Enterprise Firewall Release Notes* for issues related to feature support for the current version or corrections to documentation. Check the Symantec Web site (www.symantec.com/techsupp/) for the latest updates to all products.

## Intended audience

This manual is intended for system managers or administrators responsible for installing the Symantec Enterprise Firewall. Installers should have a solid grounding in internetworking concepts and experience installing software on Windows 2000/2003 systems or Sun Solaris 8 or 9 operating systems.

## Document structure

This manual is structured as follows:

**Table 1-1** Document structure

| Chapter | Title | Content |
|---|---|---|
| Chapter 2 | Installing the security gateway on Microsoft Windows server | Contains instructions for installing the security gateway software on Microsoft Windows operating system. |
| Chapter 3 | Installing the security gateway on Sun Solaris 8 or 9 server | Contains instructions for installing the security gateway software on Sun Solaris 8 or 9 operating system. |
| Chapter 4 | Using the System Setup Wizard | Instructions on how to run the System Setup Wizard for upgrades, restores, and first-time configurations. |
| Chapter 5 | Verifying your installation | Verifies your installation has completed properly. |
| Appendix A | Developing a pre-installation security plan | Lays out basic guidelines for developing an overall security plan and provides a checklist for assessing your security issues. |
| Appendix B | Licensing | Defines the basic licensing requirements and policies. |

**Table 1-1** Document structure (Continued)

| Chapter | Title | Content |
|---|---|---|
| Appendix C | Troubleshooting | Contains information for how to access the most up-to-date troubleshooting information for the Symantec Enterprise Firewall. |

## Developing a security plan

Before you install, you should have developed a security plan. Developing a security plan is the most important piece of the installation process. Appendix A provides an outline for developing your security policy and a checklist for gathering the information you need to facilitate the installation process.
See "Developing a pre-installation security plan" on page 65.

During this process, you gather the required IP addresses that make your installation process a success.

# Managing your client environment

The Symantec Enterprise Firewall supports management from different platforms through the SGMI. You can access the SGMI with a client computer and a supported browser, such as Microsoft Internet Explorer version 6 or later or Netscape Navigator version 7 or later.

**Note:** You must disable the browser feature that auto-saves passwords. This could compromise security. Generally, this is a default browser setting.

## Java Runtime Environment

There are supported versions of the Java Runtime Environment (JRE) for specific browsers. For the browser to process Java, a JRE is required. A JRE is downloaded automatically the first time the Security Gateway Management Interface (SGMI) is run.

**Note:** These JRE versions relate only to the client or browser side. The security gateway uses JRE 1.3.1_04.

Refer to Table 1-2 for the appropriate JRE version for your browser.

**Table 1-2** Browser and Java support

| Application | Version | Java Runtime Environment (JRE) |
|---|---|---|
| Microsoft Windows Internet Explorer | 6 or later | JRE 1.3.1_04 or later |
| Windows Netscape | 7 or later | JRE 1.3.1_04 or later |
| Solaris Netscape | 7 or later | JRE 1.4.2 or later |

In addition, ensure that your client computer has a minimum of 512 MB of random access memory (RAM).

## Microsoft Windows hardware and software requirements

Table 1-3 shows the hardware requirements for the security gateway for a Microsoft Windows environment.

**Table 1-3** Microsoft Windows hardware requirements

| Component | Requirements | Comments |
|---|---|---|
| Network interface cards (NICs) | A minimum of two network interface cards from the Microsoft Hardware Compatibility List (HCL) for the following media types:<br>■ Ethernet<br>■ FastEthernet<br>■ Gigabit Ethernet<br>■ Ethernet Fiber<br>See "Supported network interface cards (NICs) in High Availability/Load Balancing mode" on page 15. | Configure for TCP/IP and with static IP addresses. You must enable and connect adapters to a switch or hub, prior to installing and running the System Setup Wizard.<br>Check the Microsoft Web site at www.microsoft.com. |
| CPU | Sites with less than 200 users: Intel Pentium III 800 MHz<br>Sites with more than 200 users: Intel Pentium III 1.2 GHz | Maximum of four CPUs. |

**Table 1-3** Microsoft Windows hardware requirements (Continued)

| Component | Requirements | Comments |
|---|---|---|
| Memory (RAM) | Sites with less than 200 users: 512 MB<br>Sites with more than 200 users: 1 GB | More memory is recommended depending on resource usage. |
| Disk space | Sites with less than 200 users: 10 GB disk with at least 512 MB paging file<br>Sites with more than 200 users: 15 GB disk with at least 1 GB paging file | Symantec Enterprise Firewall installations require at least 200 MB for configuration and log files. |

Table 1-4 shows the Symantec Enterprise Firewall software requirements.

**Table 1-4** Microsoft Windows software requirements

| Component | Requirements | Comments |
|---|---|---|
| Operating systems | One of the following:<br>■ Microsoft Windows Server 2000<br>■ Microsoft Windows Advanced Server 2000<br>■ Microsoft Windows Server 2003 Standard Edition | Windows 2000 Service Pack 4 (SP4). Check the Symantec Web site at www.symantec.com for updates. |
| Client browser requirements<br>(for SGMI) | Microsoft Explorer 6 or later<br>Netscape Navigator version 7 or later<br>A computer with 256 color display and set to 1024 x 768 maximum. | Microsoft Explorer 6.0 is included with Microsoft Windows 2000 and 2003.<br>The SGMI can be run on the firewall or from a separate computer. |

# Sun Solaris hardware and software requirements

The hardware requirements for Sun Solaris are shown in Table 1-5.

**Table 1-5** Sun Solaris hardware requirements

| Component | Requirements | Comments |
|---|---|---|
| CPU | Supports 32-bit operation on Sun Microsystems SBUS and PCI architecture workstations or servers based on UltraSPARC II, and UltraSPARC IIi processors.<br>Supports 64-bit operation on Sun Microsystems SBUS and PCI architecture workstations and servers based on the UltraSPARC II, UltraSPARC IIi, UltraSPARC IIe, UltraSPARC III, UltraSPARC III Cu, and UltraSPARC III+ processors.<br>Sites with less than 200 users: 600 MHz.<br>Sites with more than 200 users: 1 GHz. | Single and multi-processor systems are supported. Check the Symantec Web site at www.symantec.com for recommended Sun Solaris patches. |
| Memory (RAM) | Sites with less than 200 users: 512 MB.<br>Sites with more than 200 users: 1 GB. | More memory is recommended. |
| Disk space | Sites with less than 200 users: 10 GB disk with swap space equal or greater to RAM.<br>Sites with more than 200 users: 15 GB disk with swap space equal or greater to RAM. | The Symantec Enterprise Firewall installation requires at least 500 MB for its configuration and log files. |

**Table 1-5** Sun Solaris hardware requirements (Continued)

| Component | Requirements | Comments |
|---|---|---|
| Datalink driver | Sun's be, bge, ce, eri, ge, hme, nf, qe, qfe, tr<br>Fore's fore_atm (in LAN emulation and CLIP mode)<br>SysKonnect's skge<br>Znyx's znb | For updates and the most current driver recommendations, refer to:<br>http://www.symantec.com/techsupp/enterprise/select_product_kb.html<br>Type this document ID: 2003112019183954, and then clikc the Go button. |

Table 1-6 shows the Sun Solaris software requirements.

**Table 1-6** Sun Solaris software requirements

| Component | Requirements | Comments |
|---|---|---|
| Operating systems | Sun Solaris 8 (32 and 64-bit).<br>Sun Solaris 9 (64-bit). | |
| Client browser requirements (for SGMI) | Microsoft Explorer 6 or later.<br>Netscape Navigator version 7 or later. | Microsoft Explorer 6.0 is included with Microsoft Windows 2000 and 2003.<br>The SGMI can be run on the firewall or from a separate computer. |

The Symantec Enterprise Firewall does not support RAID level 0 (disk mirroring).

## Supported network interface cards (NICs) in High Availability/Load Balancing mode

The tables below provide details of supported NICs in HA/LB mode for Microsoft Windows or Sun Solaris operating systems. Check the Symantec Web site at www.symantec.com or your *Symantec Enterprise Firewall Release Notes* for updates.

## For Microsoft Windows

Table 1-7 shows the datalink drivers that are supported in an HA/LB environment.

**Table 1-7** Supported Microsoft Windows datalink drivers in an HA/LB environment

| NIC | Comments |
|---|---|
| SysKonnect Gigabit Ethernet SK-9821 V2.0 | For updates and the most current HA/LB driver recommendations refer to:<br>http://www.symantec.com/techsupp/enterprise/select_product_kb.html<br>Type this document ID: 2003112019183954, and then clikc the Go button. |
| 3Com EtherLink Server NICs (3C980/3C980B/3C980C) | |
| Intel PRO/100 S and PRO/100+ Family of Fast Ethernet Desktop and Server Adapters | |
| Intel PRO/1000 Family of Gigabit Desktop and Server Adapters | |
| Broadcom NetExtreme BCM5700 Gigabit Ethernet Adapter | |
| Adaptec DuraLAN Fast Ethernet Quartet 66 (ANA-64044) and Quartet 64 (ANA-62044) quad-port NICs | |

### For Sun Solaris 8 and 9

Table 1-8 shows the datalink drivers that are supported in an HA/LB environment.

**Table 1-8** Sun Solaris supported datalink drivers in an HA/LB environment

| NIC | Comments |
|---|---|
| SysKonnect Gigabit Ethernet SK-9821 V2.0 | For updates and the most current driver recommendations refer to:<br>http://www.symantec.com/techsupp/enterprise/select_product_kb.html<br>Type this document ID: 2003112019183954, and then clikc the Go button. |
| Onboard Broadcom Gigabit Ethernet Interface | |
| Sun Fast Ethernet and Sun SunSwift | |
| Sun Quad FastEthernet | |
| Sun Gigabit Ethernet | |
| Sun GigaSwift Ethernet | |

## Understanding your installation options

Before you install your security gateway software, you need to determine which installation path to take. Table 1-9 defines each of the three installation options.

**Table 1-9** Installation options

| Install type | Definition | Uninstall previous version? | Restore previous configuration? |
|---|---|---|---|
| First time | You are installing the security gateway for the first time. | No | No |
| Upgrade | You are installing the 8.0 version of the security gateway on a computer that ran the 7.x version. | Yes* | Yes, from the backup file of the saved 7.x configuration. |
| Backup and restore | You are installing the security gateway on a new computer using a saved or archived configuration file. | No | Yes, from the backup file of the saved 7.x or 8.0 configuration. |

* If you are upgrading, you must apply all the hotfixes between your release version and Symantec Enterprise Firewall version 8.0, back-up and password-protect your 7.x configuration files according to the directions for that version, and uninstall your previous security gateway software before installing the new version. You cannot upgrade between platforms.

# Where to get more information

The Symantec Enterprise Firewall functionality is described in the following manuals:

- *Symantec™ Enterprise Firewall Installation Guide*
  The guide you are reading covers the physical installation and initial setup of the security gateway, licensing, and the SGMI.
- *Symantec™ Enterprise Firewall Administrator's Guide*
  This guide covers configuration topics related to the security gateway and its related components, including: the SGMI, base components, access controls, secure tunnels, VPN policies, remote policies, and monitoring controls. It is provided in PDF format.
- *Symantec™ Security Gateways Reference Guide*
  This guide provides advanced technical information about configuring network security and advanced configuration examples for Symantec security gateways.
- *License Organizer*
  This document provides useful information for obtaining license files.
- *Symantec™ Enterprise Firewall Release Notes*
  This document provides additional information on supported features or corrections to documentation.

# CD-ROM layout

To help you understand where to find the files you need to install on your computer, the CD-ROM layout for both the Microsoft Windows and Sun Solaris versions of the software are documented in this section.

## For Microsoft Windows operating systems

The volume label name of the Symantec Enterprise Firewall Microsoft Windows version CD-ROM is SEF_WINDOWS_8_0. This CD-ROM includes the following files:

ClientSoftware\

Adobe\

Windows\
AdbeRdr60_emu_full.exe

SNMP\
snmpv1.mib

snmpv2.mib

RemoteTools\
linux-remtools.tgz

solaris-remtools.tgz

windows-remtools.zip

Documentation\
SEF_Installation.pdf

SEF_Administrators.pdf

SSG_Reference.pdf

SEF_ReleaseNotes.pdf

SYMC_FW\

Firewall
software
(setup.exe)

## For Sun Solaris operating systems

The volume label name of the Symantec Enterprise Firewall Sun Solaris version CD-ROM is sef_solaris_8_0. This CD-ROM includes the following files:

ClientSoftware/

Adobe/

Solaris/
solaris-507.tar

Windows/
AdbeRdr60_emu_full.exe

RemoteTools/
linux-remtools.tgz
solaris-remtools.tgz
windows-remtools.zip

SNMP/
snmpv1.mib
snmpv2.mib

Documentation/
SEF_Installation.pdf
SEF_Administrators.pdf
SSG_Reference.pdf
SEF_ReleaseNotes.pdf

SYMC_FW/
SYMCsef

# Replacement CD-ROMs

You may need to replace the media due to a defective or lost CD-ROM. If you need a replacement CD-ROM because it is defective, contact Symantec Customer Support.

If you require a new CD-ROM because you have lost it, contact your sales representative to purchase a new media kit.

Chapter 2

# Installing a security gateway on a Microsoft Windows server

This chapter includes the following topics:


- Before you install
- Installing the Symantec Enterprise Firewall version 8.0 software


## Before you install

This chapter covers how to install a Symantec Enterprise Firewall on a Microsoft Windows server.

Before you install your security gateway software you must configure your Microsoft Windows operating system settings.

### Configuring your Microsoft Windows operating system

There are several Microsoft Windows-related tasks to perform prior to installing your security gateway:

- Configuring your Microsoft Windows settings
- Verifying your Microsoft Windows network configuration

This section describes the network settings required to run security gateway and the processes for configuring them on Microsoft Windows.

Network hardening is applied by the security gateway software installation. To protect your network from the vulnerability of attack during installation, many

services are disabled when you install the security gateway. To view the services that are disabled, look in your Control Panel > Administrators> Services folder.

Before you install your security gateway, you must configure the following settings on your Microsoft Windows server. Refer to your Microsoft documentation to complete the following tasks:

- Check your network settings to confirm that the TCP/IP protocol is installed and bound to all network adapters.
- Dynamic Host Configuration Protocol (DHCP) addresses are not used by the security gateway. Never configure an adapter in the security gateway to use DHCP to assign any of its IP addresses.
- Set your system's Windows name.
  The spelling of the computer name, the TCP/IP host name, and the host name in the hosts file must match (case does not matter).
- Set your system's TCP/IP options.
- Verify the IP addresses of your network interface cards (NICs).
  The security gateway system requires at least two NICs. You must connect all NICs to different subnets. Each NIC can only have one physical IP address assigned.
  Install your network adapters using the TCP/IP protocol only. If you must disable a NIC, remove the driver for that NIC.
- Check your routing tables by doing the following:
  - Assign only one default gateway for the system.
  - The network adapter or adapters on your internal (inside) network must not have a default gateway assigned**.**
  - Configure all (permanent) static routes so that the system can reach all hosts on your inside and outside networks.
  - Ensure that a default gateway for the outside interface is assigned.

For interfaces to be recognized during the installation process, you must configure the interfaces you want to use by connecting them to a hub, switch, or loopback connector prior to installation.

### Configuring DNSd

Use the following procedure to configure DNSd.

#### To DNSd

- Point your resolver to the localhost (the loopback address 127.0.0.1).
  This is entered automatically as the first address in the DNS search order list when the security gateway is installed, so it does not require any action on your part prior to installation.

Do not remove the loopback address from the list of DNS server addresses on the DNS tab of the Advanced TCP/IP Settings window. If the loopback address is accidentally removed, you can restore it on the TCP/IP properties page.

## Verifying your network configuration

Ensure your Microsoft Windows network is working before you install your security gateway. After the product is installed, testing network connectivity and tracking down the source of any problems is more complicated.

#### To verify the TCP/IP settings

- Run ipconfig /all to verify the IP addresses and netmasks for each network interface.

---

**Note:** Windows will disable the interface if it is not plugged in.

---

#### Using the PING command

You can use the PING command to verify your network connectivity, providing that PING is not restricted by your ISP or in an access control list (ACL) on an intermediary router.

- Test an inside interface IP address with PING from the computer on which you install the product. If this fails, check the following:
  - TCP/IP may not be working properly.
  - The network adapter may be misconfigured or defective.
- Test an inside host on the same subnet as the security gateway with the PING command. If this fails, check the following:
  - The security gateway may not be properly connected to the network. Check that both ends of the cable are connected or try another cable.

- The network adapter may be defective or misconfigured (configured to use thinnet instead of twisted-pair).
- The system that you are testing with may not be running or connected to the network.

- Test a host on each separate inside non-local subnet with the PING command.
  Before attempting to ping an inside subnet, add the static route to the security gateway using the ROUTE command. If this fails, check the following:
  - The routing information on the system may be incorrect.
  - The router may not be configured properly. PING the router to verify that it is running.
  - The remote system may not be running, connected to the network, or configured properly. Check its default gateway setting. Try to PING another host on that subnet.
  - The router may be filtering packets. Try to connect by way of FTP or Telnet. If you receive a connection refused or a connect failed message within 10 seconds, then a connection was probably made (and refused).
- Test the IP address of the security gateway's outside interface with the PING command. If this fails, check the following:
  - TCP/IP may not be properly bound to that network adapter.
  - The network adapter may be misconfigured or defective.
- Test a host or router on the local outside network with the PING command. If this fails, check the following:
  - The system may not be properly connected to the network. Check both ends of the cable.
  - The network adapter may be defective or misconfigured.
  - The system that you are testing with may not be running or connected to the network.
- Test the host with the PING command.
  From other systems on the network, PING the security gateway's host. If the security gateway can PING a host, that host should be able to PING the security gateway.

If there are more than two interfaces in your security gateway, make sure you test each interface by doing the following:

- PING the interface by IP address.
- PING a host on the same subnet as the interface and on each subnet behind the interface by IP address (inside interface) or PING a host on the Internet by IP address (outside interface).

## Upgrading from Symantec Enterprise Firewall 7.x to Symantec Enterprise Firewall 8.0

**Note:** Upgrading from versions prior to 7.x requires you to upgrade to 7.x before upgrading to 8.0.

If you are upgrading, you must apply all the hotfixes between your release version and Symantec Enterprise Firewall version 8.0, back-up and password-protect your 7.x configuration files according to the directions for that version, and uninstall your previous security gateway software before installing the new version.

**Warning:** You cannot upgrade between platforms. For example, you cannot restore a Microsoft Windows backup file on a Sun Solaris computer.

Before you uninstall a previous version of the security gateway software, always check the Symantec Web site for the latest version of *Symantec Enterprise Firewall Release Notes* with uninstall instructions for that version of the product.

### To upgrade from Symantec Enterprise Firewall 7.x to Symantec Enterprise Firewall 8.0

1. To back up and uninstall your Symantec Enterprise Firewall 7.x, see the administrator's guide for that release and the associated Symantec Enterprise Firewall Release Notes.
2. To install and set up Symantec Enterprise Firewall 8.0 with a backup configuration file, see "Running the System Setup Wizard to restore a previous configuration" on page 40.

**Warning:** Before you create your 8.0 configuration, clear your browser cache.

# Installing the Symantec Enterprise Firewall version 8.0 software

Before beginning the security gateway software install, refer to the Symantec Enterprise Firewall Release Notes for important information regarding installation and upgrades. Always check the Symantec Web site (www.symantec.com) for the latest information. Ensure that the partition for log files is at least 512 MB. After the security gateway is installed on the computer, point to it from your client computer with a supported browser to run the System Setup Wizard.

Before you install the security gateway, do the following:

- Clear your browser cache.
- Uninstall IPX if necessary. (Do not reinstall. Remove any protocols other than TCP/IP.)
- Physically attach to the network.

### To configure your initial network

1. Log on to the server as the local administrator or as a user in the Local Admin group.
2. Insert the *Symantec Enterprise Firewall* distribution CD-ROM.
3. Browse to the following folder:
   SYMC_FW
4. Double-click **Setup.exe**.
   The Install Shield wizard launches.
5. In the Welcome to Setup panel, click **Next**.
6. In the License Agreement panel, read the agreement carefully, and then do one of the following:
   - To accept the terms of the license agreement, click **Yes**.
   - To decline the terms of the license agreement and quit setup, click **No**.
7. Click **Next**.
8. In the Destination Drive panel, select the destination drive.
9. Click **Next**.

10 In the Install Selected Components panel, review the selected components, and then do one of the following:
   - If you agree with the selected components, click **Next**.
   - If you do not agree with the selected components, click **Back** to make changes, and then click **Next**.
     In the Setup Status panel, an install bar indicates the progress of your installation.
11 In the Management Password panel, do the following:
   - In the Password text box, type the password.
     You use this password to log on to the SGMI.
   - In the Verify Password text box, type the password again.
12 Click **Next**.
13 In the Setup Complete panel, do one of the following:
   - To restart the computer now, click **Yes**.
   - To restart the computer later, click **No**.
     If you click No, the security gateway may not run properly until you reboot it.

## Installing RemoteLog

Install RemoteLog to allow secure access to log files for log analysis. The required self-extracting files (windows-remtools.zip), are located on the *Symantec Enterprise Firewall* CD-ROM in ClientSoftware\RemoteTools\.

This utility has been modified to read the binary log files and to translate them into English. The Flatten8 utility has been extended to flatten all messages. RemoteLog utilities are not backwards compatible, and the installation CD-ROM includes both the version 7.0 and 8.0 RemoteLog utilities.

---

**Warning:** Do not install the remotelog client on the Symantec Enterprise Firewall. Doing so overwrites the remotelog server with the remotelog client.

---

For more information on using RemoteLog, see the Readme file on the *Symantec Enterprise Firewall* CD-ROM.

## Using Vulture to disable unauthorized services

The Vulture program detects and disables services running on the Symantec security gateway that do not meet the following requirements:

- Required by the security gateway.

- Part of the security gateway software.
- Specified in the vulture.runtime file.
- Running on behalf of a user not specified in the vulture.runtime (any process running on behalf of a user that is not specified is also stopped).

In addition, Vulture detects and logs out any user that is not defined in vulture.runtime.

---

**Note:** Do not run software other than Symantec Enterprise Firewall on the security gateway computer including scripts, batch files, and third-party software. Symantec does not support third-party software running on the security gateway computer. Symantec Technical Support requires the removal (not just disablement) of all third-party software prior to troubleshooting any issues.

---

### To configure Vulture

By default, the Vulture's activation frequency is one minute. You can change this frequency in the SGMI, in the System folder, on the Advanced tab.

#### To define elapsed time (in seconds) for scanning

- In the SGMI, on the Advanced tab, on Advanced Options, use the Option Name vultured.elapsetime to define the elapse time (in seconds) for scanning.
  A value of -1 disables Vulture.

#### To define allowed users that start processes

- In the SGMI, on the Advanced tab, on Advanced Options, use the Option Name vultured.users to define users allowed to start processes.
  You can exempt user accounts and server applications from Vulture on an individual basis.

#### To define additional services that are allowed to run

- In the SGMI, on the Advanced tab, on Advanced Options, use the Option Name vultured.services to define services you do not want stopped.

Chapter 3

# Installing the security gateway on a Sun Solaris 8 or 9 server

This chapter includes the following topics:


- Before you install
- Installing the Symantec Enterprise Firewall version 8.0 software


## Before you install

This chapter provides instructions for installing on a Solaris 8 (32-bit or 64-bit mode) or Solaris 9 (64-bit mode only) operating system.

Before you install you must configure and verifying the Solaris operating system settings.

### Configuring your Solaris operating system

Prior to installing the Solaris version of the security gateway, you need to configure your Solaris operating system, and then verify that it works.

The following network setting parameters are for the Solaris 8 and 9 platforms only. Use this checklist prior to installing your security gateway.

- Ensure you install all network adapters correctly and that they have the latest versions of their drivers. For a list of supported NICs, see "Supported network interface cards (NICs) in High Availability/Load Balancing mode" on page 15.

- Ensure that the TCP/IP protocol and network connectivity are working properly. All interfaces must have unique IP addresses on their respective subnets.
- Check your routing tables.
- There should be exactly one default route assigned for the system, typically pointing to your Internet router.
- Configure all static (permanent) routes so that the system can reach all hosts on your inside and outside networks.
- Edit the file called /etc/rc2.d/S70staticroutes and add routes using the route add command. This is the file that the GUI looks for to manage the routes. Once this is done, you should be able to reach both external hosts and all of the computers on your inside networks.

  For performance reasons, configure as few static routes as possible.
- Verify the host name.

  The /etc/nodename file should contain the system name only. Do not use a period (.) within the name. Do not include its domain name.

  For example, if your host's fully qualified domain (FQDN) name is firewall.corp.symantec.com, put firewall in the /etc/nodename file. Do not put firewall.corp.symantec.com or firewall.corp. in the /etc/nodename file.
- Ensure that the /etc/hosts file has an entry that maps the FQDN (using host name from /etc/nodename and domain from /etc/resolv.conf) to the primary IP address. The same line entry needs to have an alias loghost and an alias being mapped to the device name file.

  For example if the device hme0 has an IP address of 192.168.102.1 and /etc/hostname.hme0 has an entry fw1 then /etc/hosts needs to have a line that looks like this:

  ```
  192.168.102.1 firewall.corp.symantec.com fwl loghost
  ```

  You can use any alias for this host entry, but at least you need to have fw1. The file also needs a properly formatted localhost line. For example, if the DNS host name of the security gateway is thesg, the domain name is noadsorspam.com, and the IP address of the inside network interface is 10.1.2.3, the /etc/hosts file must contain the following lines:

  ```
  127.0.0.1 localhost
  10.1.2.3 thesg.noadsorspam.com thesg loghost
  ```

  The Solaris syslog depends on a loghost existing on a system interface. Ensure you have an entry in /etc/hosts for each network interface device you want to enable before installing the firewall product.
- Know the IP addresses of your Domain Name System (DNS) servers.

  If you have an internal DNS server for your site, configure the DNS Search Order in /etc/resolv.conf to use it first.

Ensure /etc/resolv.conf has the domain line using the domain only.
For example:

```
domain corp.symantec.com
```

- Check the /etc/nsswitch.conf file to ensure that the DNS switch is enabled.
  For example:

```
hosts: files dns
```

# Verifying UNIX TCP/IP settings

Use the following procedure to verify your UNIX TCP/IP settings. This is only for Sun Solaris 8 or 9 systems.

### To verify the UNIX TCP/IP settings

1. From a terminal session on Solaris, run ifconfig -a.
2. To verify that your routing table is correct, run netstat -nr.

## Using the PING command

You can use the PING command to verify your network connectivity, providing that PING is not restricted by your ISP or in an access control list (ACL) on an intermediary router.

- Test an inside interface IP address with PING from the computer on which you install the product. If this fails, check the following:
  - TCP/IP may not be working properly.
  - The network adapter may be misconfigured or defective.
- Test an inside host on the same subnet as the security gateway with the PING command. If this fails, check the following:
  - The security gateway may not be properly connected to the network. Check that both ends of the cable are connected or try another cable.
  - The network adapter may be defective or misconfigured (configured to use thinnet instead of twisted-pair).
  - The system that you are testing with may not be running or connected to the network.
- Test a host on each separate inside non-local subnet with the PING command.
  Before attempting to ping an inside subnet, add the static route to the security gateway using the ROUTE command. If this fails, check the following:
  - The routing information on the system may be incorrect.

- The router may not be configured properly. PING the router to verify that it is running.
- The remote system may not be running, connected to the network, or configured properly. Check its default gateway setting. Try to PING another host on that subnet.
- The router may be filtering packets. Try to connect by way of FTP or Telnet. If you receive a connection refused or a connect failed message within 10 seconds, then a connection was probably made (and refused).

- Test the IP address of the security gateway's outside interface with the PING command. If this fails, check the following:
  - TCP/IP may not be properly bound to that network adapter.
  - The network adapter may be misconfigured or defective.
- Test a host or router on the local outside network with the PING command. If this fails, check the following:
  - The system may not be properly connected to the network. Check both ends of the cable.
  - The network adapter may be defective or misconfigured.
  - The system that you are testing with may not be running or connected to the network.
- Test the host with the PING command.
  From other systems on the network, PING the security gateway's host. If the security gateway can PING a host, that host should be able to PING the security gateway.
  If there are more than two interfaces in your security gateway, make sure you test each interface by doing the following:
  - PING the interface by IP address.
  - PING a host on the same subnet as the interface and on each subnet behind the interface by IP address (inside interface) or PING a host on the Internet by IP address (outside interface).

## Upgrading from Symantec Enterprise Firewall 7.x to Symantec Enterprise Firewall 8.0

**Note:** Upgrading from versions prior to 7.x requires you to upgrade to 7.x before upgrading to 8.0.

If you are upgrading, you must apply all the hotfixes between your release version and Symantec Enterprise Firewall version 8.0, back-up and password-

protect your 7.x configuration files according to the directions for that version, and uninstall your previous security gateway software before installing the new version. You cannot upgrade between platforms.

Before you uninstall a previous version of the product, always check the Symantec Web site for the latest version of release notes with uninstall instructions for that version of the product.

### To upgrade from Symantec Enterprise Firewall 7.x to Symantec Enterprise Firewall 8.0

1. To back up and uninstall Symantec Enterprise Firewall 7.x, see the administrator's guide for that version and the associated release notes.
2. To upgrade and set up Symantec Enterprise Firewall 8.0 with a backup configuration file, see "Running the System Setup Wizard to restore a previous configuration" on page 40.

---

**Warning:** Before you create your Symantec Enterprise Firewall 8.0 configuration, use your specific browser manufacturer instructions to clear your cache.

---

# Installing the Symantec Enterprise Firewall version 8.0 software

Before beginning the new security gateway software installation, refer to the *Symantec Enterprise Firewall version 8.0 Release Notes* for important information about installation and upgrades. Always check the Symantec Web site at (www.symantec.com) for the latest information. Ensure that the partition for log files, /usr/adm/sg, is at least 500 MB.

---

**Note:** Before beginning the installation, ensure your Solaris operating system for Solaris 8 is either in 32 or 64-bit mode. Solaris 9 is only supported in 64-bit mode.

---

### To install the Symantec Enterprise Firewall 8.0 software

1. Become superuser.
2. Insert the CD-ROM into the CD-ROM drive, and then type the following command:

```
cd /cdrom/sef_solaris_8_0
```

3 To execute the install program, type the following command:

```
pkgadd -d SYMC_FW SYMCsef
```

4 Do one of the following:

- To accept the license agreement, type the following command:

  ```
  y
  ```

- To reject the license agreement, type the following command:

  ```
  n
  ```

5 At the command prompt, type the new password for the default account (admin:).

This is the password you use later to configure the SGMI. See "Running the System Setup Wizard for initial configuration" on page 47.

If you have previously installed a security gateway, you may see the message that states that the files you want to install are being used by another package. Disregard the message.

6 To install these conflicting files, type the following command:

```
y
```

7 To continue with the installation of <SYMCsef>, type the following command:

```
y
```

For the next few minutes, you see the installation progress on your screen. When the installation completes, the screen displays:

```
Installation of <SYMCsef> was successful.
```

8 Follow the instructions on the screen to reboot your system.

After the system reboots, you are ready to proceed with the System Setup Wizard to either upgrade or restore a previous configuration or to complete your initial configuration.

See "Running the System Setup Wizard for initial configuration" on page 47.

## Installing RemoteLog

Install RemoteLog to allow secure access to log files for doing log analysis. The self-extracting files, remlog.zip, remlog.tgz, which are required for RemoteLog, are located on the *Symantec Enterprise Firewall* CD-ROM in the ClientSoftware/RemoteTools/ directory.

The Flatten8 utility has been extended to flatten all messages. RemoteLog utilities are not backwards compatible, and the installation CD-ROM includes both the 7.0 and 8.0 RemoteLog utilities.

---

**Warning:** Do not install the remotelog client on the Symantec Enterprise Firewall. Doing so will overwrite the remotelog server with the remotelog client.

---

For more information on using RemoteLog, see the Readme file on the *Symantec Enterprise Firewall* CD-ROM.

Chapter 4

# Using the System Setup Wizard

This chapter includes the following topics:


- Understanding the System Setup Wizard
- Obtaining your license file
- Upgrading or restoring your configuration from Symantec Enterprise Firewall version 7.x
- Running the System Setup Wizard to restore a previous configuration
- Running the System Setup Wizard for initial configuration


## Understanding the System Setup Wizard

You run the System Setup Wizard after installing the security gateway software. The System Setup Wizard functions exactly the same whether your security gateway is on a Microsoft Windows or Sun Solaris operating system, with some minor variations such as the drop-down menus which are platform specific. The System Setup Wizard is where you:

- Complete a first time configuration
- Upgrade the Symantec Enterprise Firewall 7.x security gateway configuration on an existing computer
- Restore a Symantec Enterprise Firewall version 7.x or 8.0 security gateway configuration on a new computer

You can run the System Setup Wizard to change any of the basic settings, which include configuring your time settings, selecting the system features you want to enable, configuring the logical network interfaces, and setting up SMTP,

HTTP, and FTP settings to get traffic flowing. You can find advanced configuration instructions in the *Symantec Enterprise Firewall Administrator's Guide*. When you finish running the System Setup Wizard, the system reboots.

You connect to the security gateway by browsing to its IP address from a client computer with a supported browser and password specified during security gateway software installation. See "Installing the Symantec Enterprise Firewall version 8.0 software" on page 33. For a detailed description of the SGMI, see the *Symantec Enterprise Firewall Administrator's Guide*.

# Obtaining your license file

With version 8.0 and later, you no longer use a license key; it has been replaced with a license file. A license file is required for your product for when you upgrade from Symantec Enterprise Firewall version 7.x to 8.0 and for the first install. The security gateway software generates an evaluation license that lets the software operate for a 30-day grace period.

**Note:** Once the 30-day grace period has expired, a permanent license file is required for the security gateway to operate.

At any point during those 30 days, use the online license file generator from the Symantec licensing and registration site at www.symantec.com/certificate to obtain a license file. If you have obtained your license files you can use the System Setup Wizard to upload them to your security gateway. See "Using the Symantec License Request & Maintenance Web site" on page 91.

**Warning:** You must take the time to plan and organize for obtaining your license.

# Upgrading or restoring your configuration from Symantec Enterprise Firewall version 7.x

In Chapter 1, you determined which type of install process you would need depending on three different options. See "Understanding your installation options" on page 17. Whether you are upgrading your software on an existing machine, or restoring a configuration to a new machine, you use the System Setup Wizard.

For a restore on a new computer, you use the backup file in a directory on the computer where the SGMI is running.

This restore begins the first time you run the System Setup Wizard.

---

**Note:** You can only accomplish the following procedure the first time you run the System Setup Wizard. The Restore from backup image check box does not display after the first use.

---

For directions on how to restore a Symantec Enterprise Firewall to a previous configuration at any point after an initial setup, see the *Symantec Enterprise Firewall Administrator's Guide*.

You can upgrade a previous configuration if you are upgrading from a supported release. Table 4-1 shows a list of supported versions. It is expected that you have already upgraded from a prior version to 7.x. Refer to your product release notes for upgrade information for a version prior to 7.0.

**Table 4-1** Supported version

| Product | Software version |
|---|---|
| Symantec Enterprise Firewall | 7.0.0 and 7.0.4 |

## Upgrading limitations

Certain functionality has limitations when migrating from a previous release. These include the following topics:

| | |
|---|---|
| Licensing | You cannot use upgraded or restored product licenses from the previous product versions. You must obtain new license files to activate the new security gateway. |
| Network interfaces | The new security gateway must have an equal or greater number of interfaces as the backup image. The upgrade cannot continue if the number of interfaces does not meet this requirement. Each interface must have a unique IP address on the respective subnet. |
| DES to 3DES/AES | DES installations are not upgraded to 3DES/AES. The product cannot change DES tunnels to 3DES tunnels because it has no control over the remote endpoint of the tunnel. The remote gateways or Client VPN users can upgrade to 3DES at a later point in time. |
| SwIPe tunnels | The upgrade deletes any SwIPe tunnels and VPN policies it finds. |
| Gopher daemon | Gopher-related configurations are not upgraded. |

| | |
|---|---|
| Crypto-card extended authentication | The Crypto-card authentication method is removed by the upgrade. |
| Finjan | Finjan related configurations are not upgraded. |
| SQL*Net | The upgrade script removes all references of SQL*Net from the configuration files. |

# Running the System Setup Wizard to restore a previous configuration

This procedure is for restoring your previous configuration. You must have Symantec Enterprise Firewall version 7.x or later and have Java Runtime Environment (JRE) v1.3.1_04 or later installed on your client computer running setup.exe. If you do not have this installed, the System Setup Wizard detects this and the Security Warning screen appears and installs the Java plug-in on the computer. You cannot continue without the Java plug-in.

Before you run the System Setup Wizard, you need the following information:

- User name (admin) and password.
- List of all the required IP addresses.
  Fill out the worksheets in Appendix A to gather your information.
- If you plan to create clusters, you need your heartbeat network interface addresses.
  The heartbeat network is the cluster management network. It is used as a private network for cluster configuration information and state. Members of a cluster communicate using the heartbeat network to provide statistical information which allows load balancing and availability.
- If you have your license files, you can upload them using the System Setup Wizard or you can use the 30-day grace period (optional) license. You can also install a license from System > Features > Installed Licenses > Install. See "Using the Symantec License Request & Maintenance Web site" on page 91.

---

**Warning:** This wizard must run through to completion to manage the security gateway. If you cancel out of this wizard without completing it, you have to run it again.

---

If you want to modify settings you set in the System Setup Wizard, rerun the System Setup Wizard from the Action menu.

---

**Note:** At the end of the System Setup Wizard, the system reboots. If you are using a system with other open applications, close all applications prior running the System Setup Wizard.

---

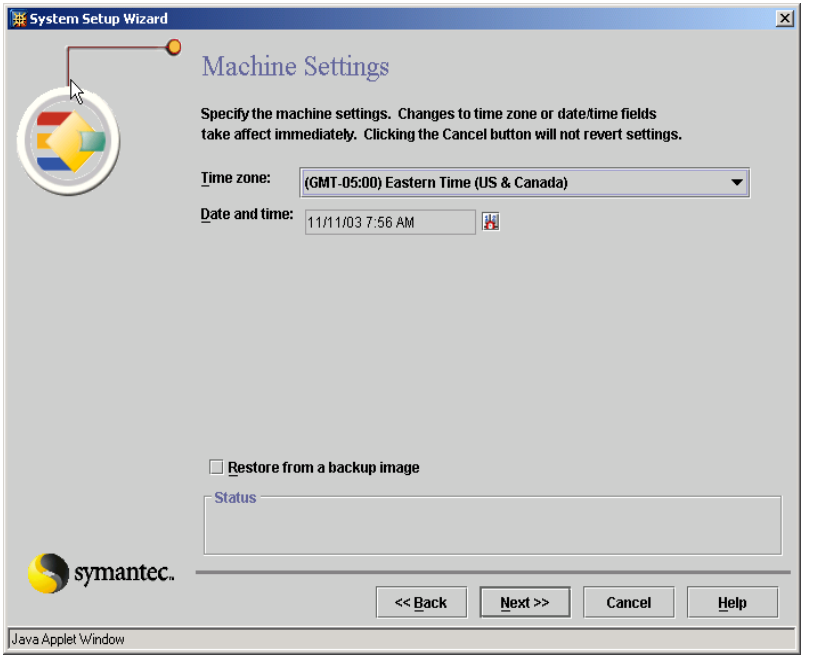
### To restore your security gateway using the System Setup Wizard

1. Before you begin the System Setup Wizard, close all other open applications. Each time you run the System Setup Wizard, the system reboots. Closing your open applications ensures you do not lose data
2. Browse to the IP address of the security gateway you want to configure. The path is:
   **https://<IP address of the security gateway>:2456/**
3. In the Security Alert panel, do one of the following:
   - To accept the certificate, click **Yes**.
     Accepting a certificate when accessing your security gateway by way of an inside (trusted) network does not present any danger. You should notate the certificate thumbprint and use it to verify the certificate thumbprint when you access your security gateway through an outside connection.
   - To view the certificate, click **View Certificate**.
   - To reject the certificate and exit the wizard, click **No**.
4. In the Log on panel, do the following:
   - In the user name box, type admin.
   - In the password box, type the administrator's password that you specified when you installed the security gateway.
5. In the License and Warranty Agreement panel, read the agreement, and then do one of the following:
   - To decline the agreement and return to the log on screen, click **Do Not Accept**.
     The System Setup Wizard does not run.
   - To accept the license and warranty agreement, and to proceed with the System Setup Wizard, click **Accept**.

The System Setup Wizard starts automatically.

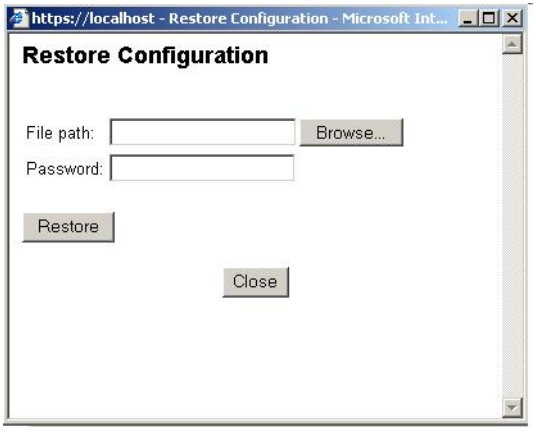
System Setup Wizard
Welcome to the System Setup Wizard
This wizard guides you through the setup of your system. You must complete this wizard. If you cancel out of the wizard without completing it, your security gateway will not be ready to operate.
symantec.
<< Back
Next >>
Cancel
Help
Java Applet Window

6 On the Welcome to the System Setup Wizard panel, click **Next**.



7 In the Machine Settings panel, do the following:

- In the Time zone drop down list, select a time zone.
- Click the icon to the right of Date and Time, and then On the Calendar panel, do the following:
  - Under Date, select the correct month, day, and year.
  - Under Time, use the drop-down list to select correct time.
    You must set the date and time. Failing to set the correct date and time could impact your product license and other product features.
  - Click **Next**.
- Check **Restore from a backup image,** and then click **Next**.
  You will not be able to cancel out of the restore process until it completes.




8 On the Restore Configuration panel, do the following:

- Browse to the location where you stored the backed up configuration.
- In the Password text box, type the password you set when you created the backup file.

9 Click **Restore**.

10 On the System Information panel, do the following:

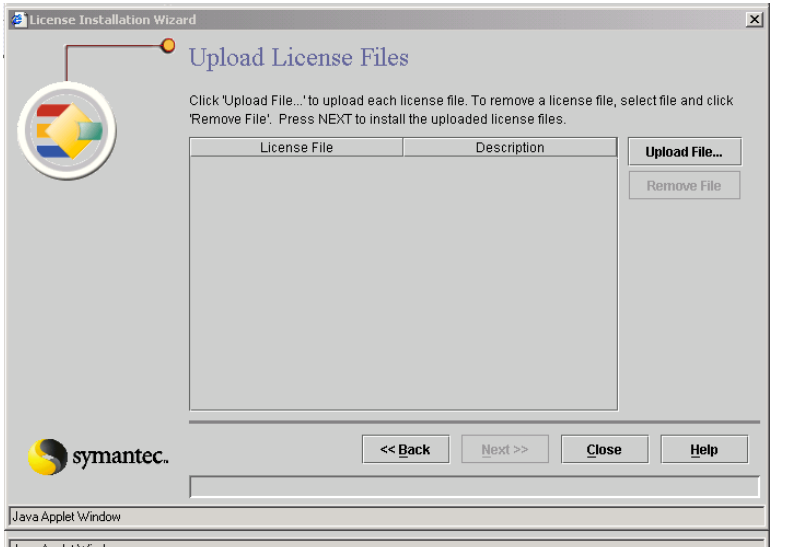
- In the Host name text box, type the host name.
- In the Domain name text box, type the domain name of the security gateway.
- In the Default gateway text box, type the default gateway IP address.

11 In the Install License Files panel, do one of the following:

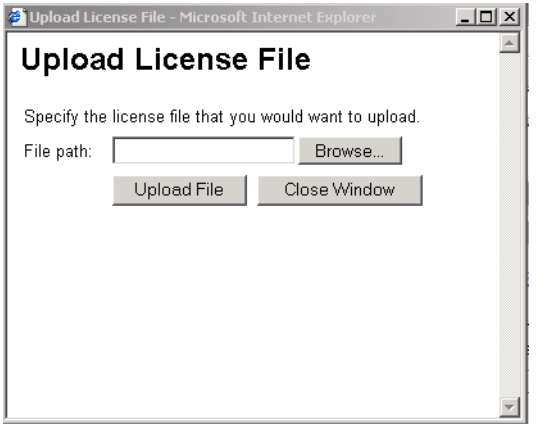
- To use the 30-day grace period and upload your license files later, click **Next**, and then skip to step 16.
- To upload your license files now, click **License Installation Wizard**, and then click **Next**.

  You must have your license files to select this option. Clicking Next initiates the License Installation Wizard.

12 On the Welcome to the License Installation Wizard panel, click **Next**.



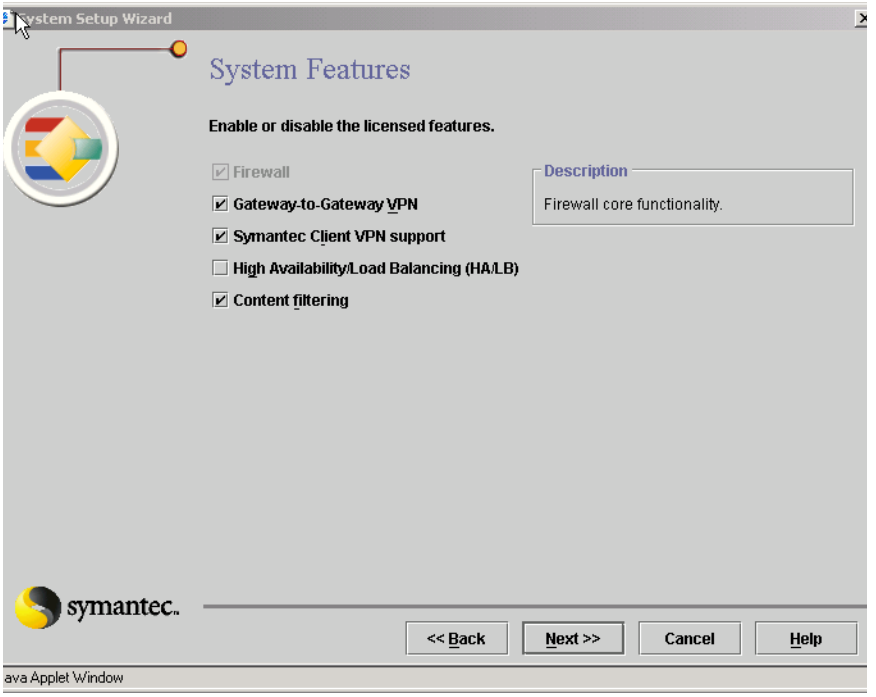

13 On the Upload License Files panel, click **Upload File**.



14 On the Upload License File panel, browse to where you have saved your license files, and then do the following:

- Select a license file, and then click **Upload File**.
- Repeat this process for all license files.
- Click **Close Window.**

15 Click **Next**.



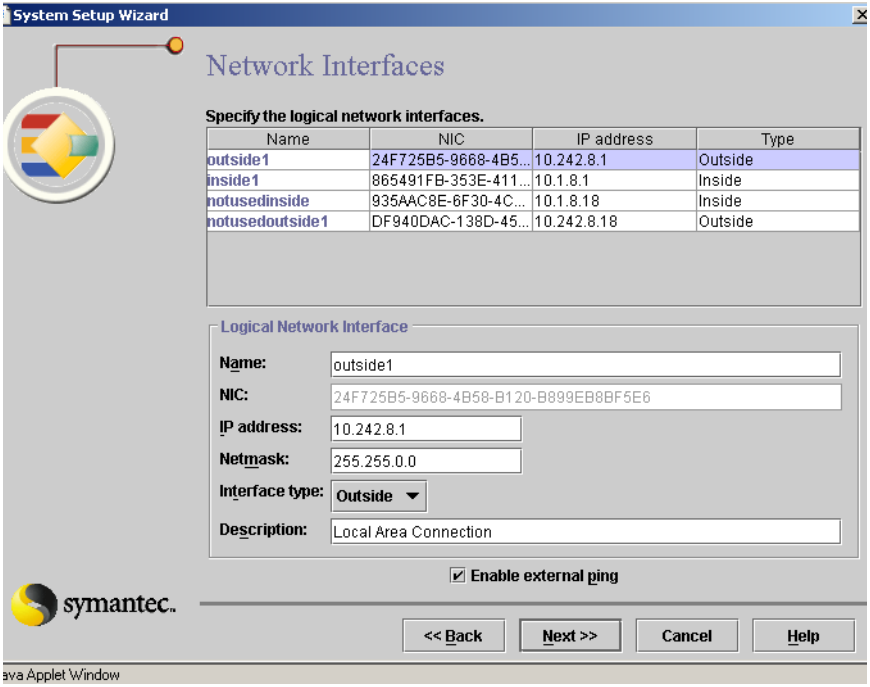

16 On the System Features panel, verify that each of the licensed features you want is enabled.

If there are features that you expected to have enabled that are not, click **Back** to ensure that you have properly loaded your license files. You must load a license file for each of the features you want enabled.

If you do not want to configure a heartbeat interface now, uncheck the check box next to High Availability/Load Balancing. If you do not uncheck this check box, you are prompted to select the heartbeat interface.

You can run the System Setup Wizard later to enable any feature, or from the SGMI, select System > Features tab > System Features to turn features on or off.

17 Click **Next**.




18 On the Network Interfaces panel, select the interfaces that you want to configure and make any necessary edits. You must name each interface and configure it for either the inside or outside interface.

If you do not name your interface or specify whether it is an inside or outside interface, a warning prompts you to complete this information before you can proceed. Do the following:

| | |
|---|---|
| Name | Type the logical network interface name. |
| NIC | What displays here depends on the platform of your system. You cannot edit this text box. |
| IP address | Edit the IP address.<br>You must use an IP address that is unique to the subnet to which it connects. |
| Netmask | Edit the netmask address. |
| Interface type | You cannot edit this drop-down list. You can designate additional interfaces as inside or outside as needed. |

| | |
|---|---|
| Heartbeat interface | If HA/LB is enabled, you must define this. You should have a dedicated private network for heartbeat communications. |
| Description | This shows operating system connection information. This is an editable field. |
| Enable external ping check box | To let external administrators issue a PING command on your security gateway, check **Enable external ping**.<br><br>**Note:** By default, PING on the external interface is disabled as a security measure. The security gateway does not respond to PING commands issued to the outside interface. If you want to enable the PING command on the external interface, do this in the System Setup Wizard. You can enable or disable the PING command after the initial configuration on the PING proxy properties window. |

19 Click **Next**.

20 In the Confirmation panel, review the summary of your configuration.

21 Click **Finish**.

When you complete the System Setup Wizard, the security gateway reboots.

Once you have completed the System Setup Wizard the first time, you can access it again in the SGMI from the Action menu and edit any system information.

# Running the System Setup Wizard for initial configuration

This section is for running the System Setup Wizard the first time when you want to complete the initial configuration of your security gateway, but are not upgrading from a previous configuration. You must have Java Runtime Environment (JRE) v1.3.1_04 or later installed on your client computer running setup.exe. If you do not have the JRE installed, the System Setup Wizard detects this and the Security Warning screen appears and installs the Java plug-in on computer. You cannot continue without the Java plug-in.

You must complete this setup procedure before you can begin managing your security gateway.

Before you begin the this setup, you need the following information:

- User name (admin) and password.
- List of all the required IP addresses.
  Fill out the worksheets in Appendix A to gather your information.

- If you plan to create clusters, you need your heartbeat network interface addresses.
  The heartbeat network is the cluster management network. It's used as a private network for cluster configuration information and state. Members of a cluster communicate using the heartbeat network to provide statistical information which allows load balancing and availability.
- If you have your license files, you can upload them using the System Setup Wizard or you can use the 30-day grace period (optional) license. See "Using the Symantec License Request & Maintenance Web site" on page 91.

This wizard must run through to completion to manage the security gateway. If you cancel out of this wizard without completing it, you have to run it again. Once you complete setup, you can run it again from the Action Menu to edit system information at anytime.

If you want to modify settings you set in the System Setup Wizard, rerun the System Setup Wizard from the Action menu.

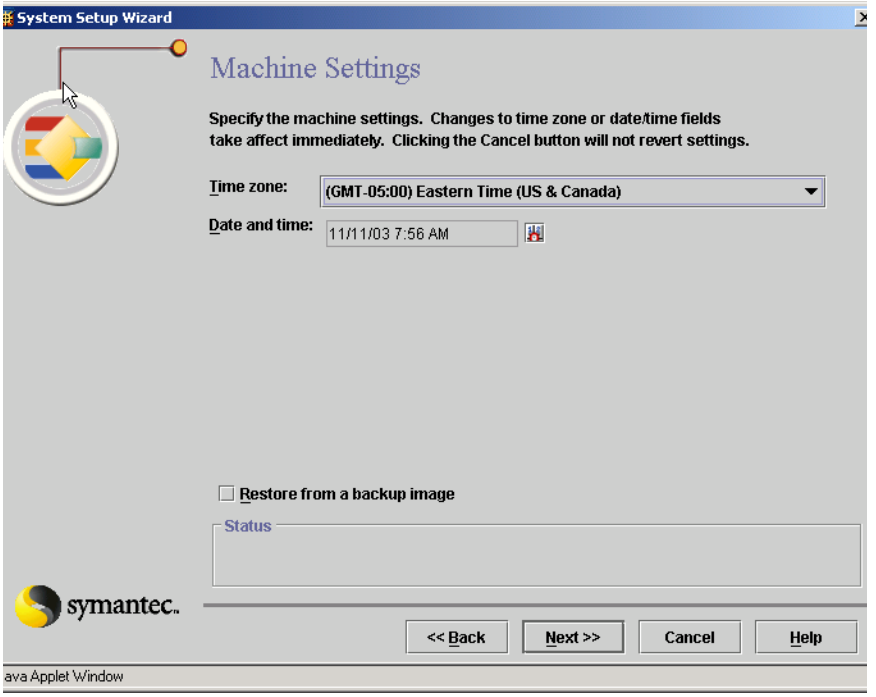
### To run the System Setup Wizard for initial configuration

1. Before you begin the System Setup Wizard, close all other open applications. Each time you run the System Setup Wizard, the system reboots. Closing your open applications ensures you do not lose data.
2. Browse to the IP address of the security gateway you want to configure. The path is:
   **https://<IP address of the security gateway>:2456/**
3. In the Security Alert panel, do one of the following:
   - To accept the certificate, click **Yes**.
     Accepting a certificate when accessing your security gateway by way of an inside (trusted) network does not present any danger. You can trust it. You should notate the certificate thumbprint and use it to verify the certificate thumbprint when you access your security gateway through an outside connection.
   - To view the certificate, click **View Certificate**.
   - To reject the certificate and exit the wizard, click **No**.
4. In the Log on panel, do the following:
   - In the user name box, type admin.
   - In the password box, type the password you received during setup.exe.

5 In the License and Warranty Agreement panel, read the agreement and then do one of the following:

- To accept the license and warranty agreement and to proceed with the System Setup Wizard, click **Accept**.
- To decline the agreement and return to the log on screen, click **Do Not Accept**.

6 On the Welcome to System Setup Wizard panel, click **Next**.




7 In the Machine Settings panel, do the following:

- In the Time zone drop down list, select a time zone.
- Click the icon to the right of Date and Time, and then On the Calendar panel, do the following:
  - Under Date, select the correct month, day, and year.
  - Under Time, use the drop-down list to select correct time.
    You must set the date and time. Failing to set the correct date and time could impact your product license and other product features.
  - Click **OK**.

- Since you are not restoring from a backup image, ignore Restore from a backup image.
- Click **Next**.

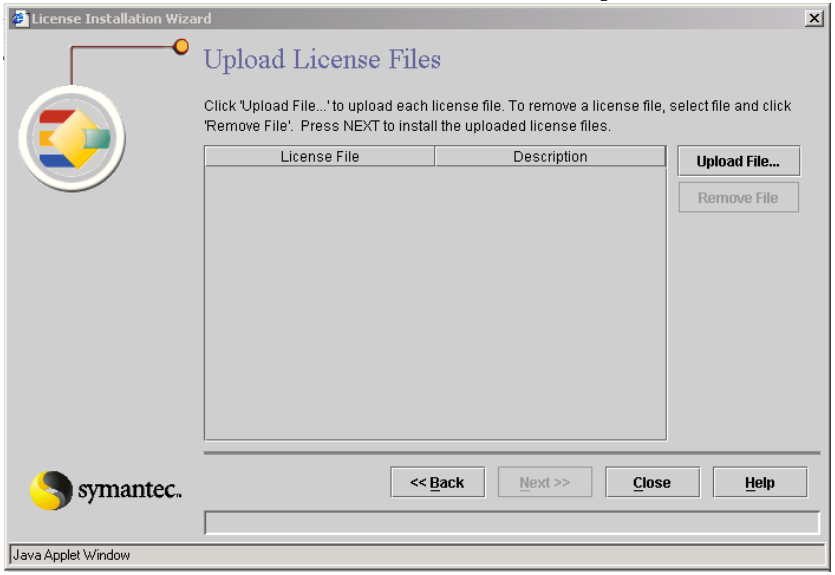
8 On the System Information panel, do the following:

- In the Host name text box, type the host name.
- In the Domain name text box, type the domain name of the security gateway.
- In the Default gateway text box, type the default gateway IP address.

9 In the Install License Files panel, do one of the following:

- To use the 30-day grace period and upload your license files later, click **Next**, and then skip to step 16.
- To upload your license files now, click **License Installation Wizard**, and then click **Next**.
  You must have your license files to select this option. Clicking Next initiates the License Installation Wizard.

10 On the Welcome to the License Installation Wizard panel, click **Next**.

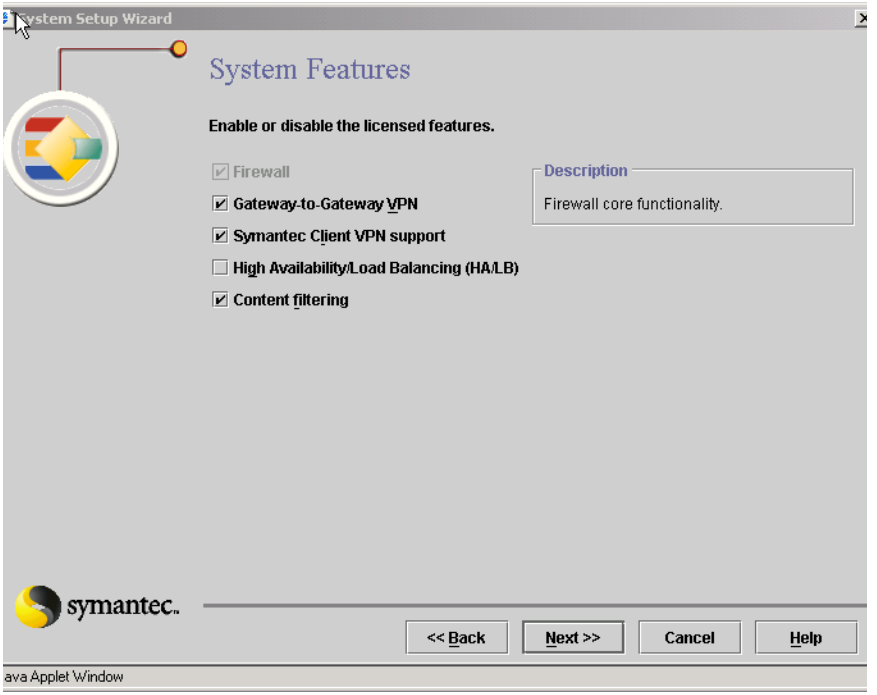


11 On the Upload License Files panel, click **Upload File**.

12 On the Upload License File panel, browse to where you have saved your license files, and then do the following:

- Select a license file, and then click **Upload File**.
- Repeat this process for all license files.
- Click **Close Window.**

13 Click **Next**.



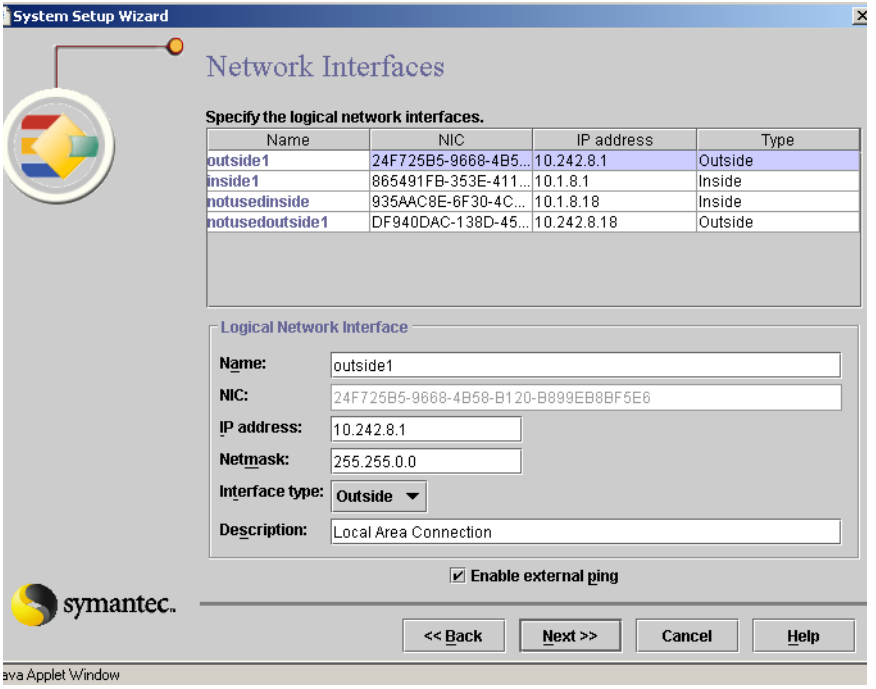

14 On the System Features panel, verify that each of the licensed features you want is checked.

If there are features that you expected to have enabled that are not, click **Back** to ensure that you have properly loaded your license files. You must load a license file for each of the features you want enabled.

If you do not want to configure a heartbeat interface now, uncheck the check box next to High Availability/Load Balancing. If you do not uncheck this check box, you are prompted to select the heartbeat interface.

You can run the System Setup Wizard later to enable any feature, or from the SGMI, select System > Features tab > System Features to turn features on or off. If you run the System Setup Wizard, the security gateway is rebooted.

15 Click **Next**.




16 On the Network Interfaces panel, select the interfaces that you want to configure and make any necessary edits. You must name each interface and configure it for either the inside or outside interface.
If you fail to either name your interface or specify whether it is an inside or outside interface, a warning pops up to prompt you to complete this information before you can proceed. Do the following:

| | |
|---|---|
| Name | Type the logical network interface name. |
| NIC | What displays here depends on the platform of your system. You cannot edit this text box. |
| IP address | Edit the IP address.<br>You must use an IP address that is unique to the subnet to which it connects. |
| Netmask | Edit the netmask address. |
| Interface type | You cannot edit this drop-down list. You can designate additional interfaces as inside or outside as needed. |

| | |
|---|---|
| Heartbeat interface | If HA/LB is enabled, you must define this. You should have a dedicated private network for heartbeat communications. |
| Description | This shows operating system connection information. This is an editable field. |
| Enable external ping check box | To let external administrators issue a PING command on your security gateway, check **Enable external ping**.<br><br>**Note:** By default, PING on the external interface is disabled as a security measure. The security gateway does not respond to PING commands issued to the outside interface. If you want to enable the PING command on the external interface, do this in the System Setup Wizard. You can enable or disable the PING command after the initial configuration on the PING proxy properties window. |

17 Click **Next**.

18 In the Optional Security Gateway Configuration panel, do one of the following:

- To configure mail, Web, and FTP services, in the Security Gateway Configuration panel, select the following:

| | |
|---|---|
| SMTP Mail services | Select this option to configure SMTP and mail services. |
| HTTP & FTP services | Select this option to configure HTTP and FTP services |

  This option only displays the first time you run the System Setup Wizard. If you choose not to configure these options now, you can configured them later with the Policy Wizard or manually by way of the SGMI Policy > Rules tab.
- If you do not want to configure these options now, then click **Next**, and then skip to step 23.

19 Click **Next**.

20 If you selected to configure mail, in the Mail Server panel, do the following:

- In the Mail server text box, type the fully qualified domain name or the IP address of the mail server.
- In the Outside IP address drop-down list, select the outside IP address for the mail server.
  You only see this option if you have more than one outside interface configured.
- Click **Next**.

21 If you selected to configure FTP and HTTP services, in the FTP and HTTP Services panel, in the Inside interface drop-down list, select the inside interface IP address.

22 Click **Next**.

23 In the Confirmation panel, review the summary of your configuration.

24 Click **Finish**.

When you complete the System Setup Wizard, the security gateway reboots.

Once you have completed the System Setup Wizard the first time, you can access it again from the Action menu and edit any system information.

## Configuring your security gateway

After you have successfully completed setup, the system reboots. When the reboot is complete, if you created rules for SMTP, HTTP, and FTP, this traffic can now pass through the security gateway. If you chose not to configure the SMTP, HTTP, and FTP traffic options, you can either use the Policy Wizard or configure it manually from the SGMI Policy > Rules tab. For more detailed instructions about how to configure these rules and how to use the Policy Wizard, see the S*ymantec Enterprise Firewall Administrator's Guide*.

# Uninstalling the security gateway software

You can uninstall the security gateway software. Use the specific directions for either Microsoft Windows or Sun Solaris.

---

**Note:** Before you uninstall, you must back up your configuration. Backup files are not interchangable across operating systems.

---

## Uninstalling the Microsoft Windows security gateway version 8.0 software

You can only attempt this after running the System Setup Wizard.

To uninstall the Symantec Enterprise Firewall version 8.0 software, run the Uninstall program. If you plan to reinstall it, you must first uninstall the software.

### To backup your configuration files

- In the SGMI, on the Action menu, select Backup.

**To uninstall the product**

- Uninstall the currently installed product using the procedures and the recommendations in the *Symantec Enterprise Firewall Release Notes*.

There are two ways to uninstall the security gateway. You can uninstall by way of Add/Remove Programs or by way of the Program Menu.

# Uninstalling the Sun Solaris security gateway 8.0 software

To uninstall the 8.0 software, run the Uninstall program. If you plan to reinstall it, you must uninstall it first.

## Unistalling the Symantec Enterprise Firewall 8.0 software

You can only attempt uninstalling after running the System Setup Wizard.

**To backup your configuration files**

- In the SGMI, on the Action menu, select Backup.

**To uninstall the Symantec software**

1. Become superuser.
2. Uninstall the Symantec product. At the command prompt type:

   ```
   pkgrm SYMCsef
   ```

   The following text displays:

   ```
   The following package is currently installed:

   SYMCsef          sef
                   (SPARC) 8.0

   Do you want to remove this package? [y,n,?,q]
   ```

3. To remove the package, at the command prompt type:

   ```
   y
   ```

   The following text displays:

   ```
   This package contains scripts which will be executed with
   super-user permission during the process of removing this
   package. Do you want to continue with the removal of this
   package [y,n,?,q]
   ```

4 To continue with the removal of the package, at the command prompt type:

```
y
```

5 Reboot the security gateway.

---

**Warning:** During installation, the security gateway copies your password file. At uninstall, it restores your password file. Except for the root password, if you have changed passwords since installation, the system reverts to the old passwords.

---

Chapter 5

# Verifying your installation

This chapter includes the following topics:


- About verifying your installation
- Checking your network card
- Managing network interface cards


## About verifying your installation

This chapter describes the procedures for verifying that you have installed your security gateway correctly. Though unlikely, it is possible to encounter problems during the installation process, such as install shell errors, missing files, or incorrect license files. In addition, you might experience problems with your basic networking or Internet connection.

If the installation fails, ensure you comply with each item in Chapter 2 or 3. Verify that your hardware is supported.

If error messages continue to appear during the installation, record the information and contact Symantec Technical Support. See "Accessing troubleshooting information" on page 107.

### Checking your basic network connectivity

Check your network connectivity. A security gateway does not pass ICMP packets unless you have a rule configured to ICMP pass packets. You cannot PING through the security gateway without configuring a rule. For information on configuring rules, see the *Symantec Enterprise Firewall Administrator's Guide*.

What PING can test:

- If you type a host name, PING first does a DNS lookup on that name.
- After it has an IP address (or if you type an address), it sends ICMP packets to see if the machine responds.
- Incorrectly installed routers cause problems. The easiest way to check routing is to use the PING utility.

You can use PING on the security gateway itself to verify connectivity. Open a command window and use the PING command to find your problem.

## PING the security gateway by address

Pinging the security gateway by address shows you if TCP/IP is installed or bound to your network interfaces.

Use the PING command to PING your inside and outside interfaces.

**Note:** By default, external PING is disabled on outside interfaces.

Each PING should return a reply. If they do not, one of the following conditions is true:

- TCP/IP is not installed
- TCP/IP is not bound to your network interfaces

**To correct the problem**

1. Uninstall the security gateway following the instructions included in this guide.
2. Install TCP/IP according to your operating system instructions. Use the most current driver.
3. Verify that you can PING these addresses.
4. Reinstall.

## PING an address on each inside network

Use the PING command to PING each inside network to show you if the specific computer is down or does not have TCP/IP installed or bound to its interface.

From a command prompt window on the security gateway, PING an address on each of the inside networks.

Each PING command should return a reply. If there is no reply, the specified computer is not on, or does not have TCP/IP installed or bound to its interface. Fix the computer and try again.

## PING more than one subnet

Use the PING command to PING more than one subnet to shows you if there is a problem between the router and the subnets.

If PING does not yield a reply, your router is turned off.

If only one of the subnets is not responding, your router is not passing ICMP. Check to see that the router is working. Check its configuration to see if it is filtering ICMP.

## Checking your Internet connection

PING your service provider connection.

If this fails, something is wrong with your connection to the Internet.

- Check your router.
- Check your service provider.
- Ping a host on the Internet. For example:

  ```
  ping www.symantec.com
  ```

If this fails:

- Use the traceroute command (tracetr <ip address>) to find out where the PING failed.
- The routing information on the system may be incorrect. Check its default gateway setting.
- You may be behind another security gateway that does not pass PING packets to the Internet.
- The router may not be configured properly.
- The remote system may not be running, connected to the network, or configured properly.
- There may be a packet filter running between your site and the other site. Try another site or try using FTP or Telnet to make the remote connection.

If all of the preceding PINGs return replies, your Internet connectivity is working.

# Checking your network card

If a machine on the Internet is unreachable, your connection to the Internet or your network card may not be working correctly or installed properly. Check the following:

- Your outside network card may not be properly installed or supported, or it may be defective. See "Supported network interface cards (NICs) in High Availability/Load Balancing mode" on page 15.
- Use the PING command to verify general network connectivity.
- Your ISP may be down or your line to the ISP may not be working.

If pinging the internal interface host name fails:

- Your name service may not be working correctly. Try pinging the same interface using the IP address instead of by name.

If you can PING a computer by address but not by name:

- You have a name service problem. Check your DNS configuration. Use the manufacturer's troubleshooting information to get your name service working.

If you cannot PING an inside system by address, then a connection is not working or there is a problem with routing.

Your inside network card may not be properly installed or supported, or it may be defective. Make sure your network card is supported. See "Supported network interface cards (NICs) in High Availability/Load Balancing mode" on page 15.

If you cannot PING a computer behind a router by address, then your static routes are incorrect, your router is not working, or the target host is not configured properly. Try the following:

- Try pinging both of the router's addresses. If you can PING the address closer to you but not the address on the other side, your router is not working or static routes are not established.
- If you can PING both addresses, the problem is with the configuration of the computer behind the router.
- If an upgrade was performed, check for interface filters.

# Managing network interface cards

With the previous version of the product, if you wanted to add/remove/change your network interface card (NIC), you had to uninstall the security gateway,

add/remove/change the NIC, and then reinstall the security gateway. With Symantec Enterprise Firewall 8.0, you no longer have to uninstall your security gateway prior to changing a NIC.

With Symantec Enterprise Firewall version 8.0, you can add/remove/change the NIC and after you reboot the computer, you only have to rerun the System Setup Wizard and verify your interfaces. After the wizard is finished, your security gateway restarts.

Appendix A

# Developing a pre-installation security plan

This chapter includes the following topics:


- About developing a security plan
- Defining your security policy
- Educating users
- Filling out worksheets


## About developing a security plan

Developing a security plan is your first step in your installation process and helps you collect the information needed to install and configure your security gateway.

## Defining your security policy

Before configuring your security gateway, you must understand exactly what network resources and services you want to protect. It is crucial to have a carefully designed network security policy to guard the valuable resources and information of your organization.

Ideally, your security policy should be captured in a document that describes your organization's network security needs and concerns. Creating this document is the first step in building an effective overall network security system and should be done prior to installation.

Your security plan details the implementation of your security policy. Based on the security concerns and trade-offs of your overall policy, your security plan

should contain a set of tasks. One of these tasks consists of establishing procedures and rules for access to resources located on your network. These resources include:

- Host computers and servers
- Workstations
- Connection devices (gateways, routers, bridges, and repeaters)
- Terminal servers and remote access servers
- Networking and applications software
- Information in files and databases

The firewall is the main tool for enforcing access rules, allowing you to define a set of "authorization rules" that allows or denies access to specific resources throughout your network.

## Before writing your security plan

Before you begin writing rules to implement your plan using the *Symantec Enterprise Firewall Administrator's Guide*, you need to answer the following questions:

- How many points of entry exist on your network?
  - A security gateway defends a single point of entry. Every point of entry should be protected by a security gateway.
  - A Virtual Private Network (VPN) server also defends a single point of entry. You must decide what access the VPN server is going to provide for resources that exist behind the firewall.
- What types of services, such as Web, FTP, and so on, do you want to allow for internal users?
- To what hosts, subnets, and users do you want to allow these services?
- What external users will have access to your network? Where will they come from and where do you want to allow them to go? During what hours? For what period of time?
- Do you intend to implement a service network?
- Do you intend to implement De-militarized zone (DMZ)?
- What types of services do you want to allow for external users and hosts?

- What type of authentication will you require for external users? (Strong authentication is recommended for any access from public networks.)
- If you are implementing VPN tunnels between any internal and external hosts, what types of traffic will be allowed over these tunnels?
- Will you place your Web server inside or outside of your protected network?

## Becoming security-conscious

Developing and implementing a security plan for the security gateway you are installing should be only one part of your overall security policy. The security gateway offers the best protection against uninvited entry into your network. However, the Symantec Enterprise Firewall cannot guard against entry by people who obtain valid authentication credentials, any more than a sophisticated lock can stop a thief in possession of the right key.

### Formulate goals

Take the time to formulate the specific goals of your security plan. Identify the resources you are protecting and all possible threats. Protecting your resources from unauthorized external users maybe only one of your goals. You may also need to limit internal access to certain systems to specific users and groups, within specific time periods. You will need to define these users and groups for the firewall and how to configure special services to be passed through these systems. The *Symantec Enterprise Firewall Administrator's Guide* explains how to define users and user groups.

### Review issues

You should review your organization's specific issues in detail before you begin configuring the server. Your network's security depends on planning sound policies, implementing them carefully, and confirming that they work as intended.

# Educating users

Your overall site policy involves a numbers of tasks. Of these, user education is paramount. Publish your company's security policy. Make sure your users are informed of the determination of would-be invaders and the sophistication of available password guessing programs. Make sure they understand how common security breaches are and how costly they can be. These facts alone dictate that users should be encouraged to select passwords that are difficult to crack and to change passwords regularly.

## Involving the user community

When developing the details of your security plan, you should solicit the input of group managers or leaders on what services they require, for what users, and so on. Explain to users the need for network security to protect private information, intellectual property, and your business plans.

### Notifying affected users

Before implementing policies, notify the user community of your proposed policies. Doing so in advance can prevent unnecessary frustration on the part of your users.

For instance, if you plan to limit Web services to a single server during specific hours, let this be known to the affected groups and users. If you plan to pass all email through a dedicated server, or if external users will be disallowed from accessing certain systems by Telnet, consider passing these changes along before implementation. Consulting users prior to implementation may save you the time needed to fine-tune those policies later.

### Taking a pro-active stance

Again, keep in mind that configuring a set of authorization rules on the security gateway is just one piece of your overall security plan. To be effective, this plan should also include:

- Physical security of key systems (especially the security gateway)
- Security risk training for users
- Guidelines on passwords
- Proprietary information policies
- Network planning

# Filling out worksheets

To aid you in the planning process, we have provided a set of policy planning worksheets. Use these worksheets to help implement the specific tasks of your security plan and to assist you during the installation process.

## Defining your organization

Begin by defining your organization. Here is where you explore your existing security policy, if any; notate who will be assigned as administrators; types of authentication; and how your administrators will be contacted.

### To define your organization

1 Does your organization have a security policy?

_____ Yes _____ No

If you checked No, refer to the first part of this chapter for information relating to the development of a security policy.

2 Number of users behind your security gateway: _____

3 Do you plan to establish special groups or users with different levels of access or control that other groups and users will not have?

_____ Yes _____ No

4 Do you plan to establish subnets, users by subnet, or users by authentication?

_____ Yes _____ No

5 What are your network access points?

_____

_____

6 Name of the primary administrator:

_____

7 Use Table A-1 to list all persons involved in administering the system.

**Table A-1** Administrator names

| Name | Email | Phone | Pager |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

**8** Are organization computer resources accessible by remote dial-in?

_____ Yes _____ No

**9** Are organization computer resources accessible by an internal network?

_____ Yes _____ No

**10** What communications servers are used? (such as SMTP or Microsoft Exchange)

_____

_____

**11** What form of authentication will be used for remote access to company resources?

_____ User name/password _____ LDAP

_____ PassGo Defender _____ RADIUS

_____ Entrust _____ Bellcore S/KEY

_____ TACACs+ _____ RSA SecurID

_____ Windows based _____ Other

**12** What mechanism will be used for suspicious activity alerts?

_____ Audio notification _____ Email

_____ Pager _____ Client program

_____ SNMP V1 _____ SNMP V2

**13** Do you have other security gateways on your network now?

_____ Yes _____ No

**14** If Yes, what brand? _____

**15** Do you have third-party firewalls on your network now?

_____ Yes _____ No

16 If Yes, which one and version? _____

17 Have you created a network diagram? If so, please print and attach.

_____ Yes _____ No

## Collecting hardware information

Before you begin the installation process, you must collect some basic hardware information.

### To collect hardware information

1 Record the Symantec System ID of the security gateway.

_____

2 Before installation, ensure the host network connections are configured and tested properly. Verify that you can PING the network interfaces of the server from clients on the same network.

3 Record the number of host computers of each type that compose your network.

_____ UNIX _____ Windows

_____ Other (type) _____

4 What kind of Internet access do you have? What speed?

_____

5 Record the name of your Internet Service Provider (ISP).

_____

6 Does your site have, or plan to have, more than one Internet access point?

_____ Yes _____ No

7 Are there any other Internet connections besides the security gateway (such as modems connected to workstations)? If yes, list.

_____ Yes _____ No

_____

_____

8 Will you be using Symantec Client VPN?

_____ Yes _____ No

## Collecting your TCP/IP address

It is important to think about the TCP/IP requirements for your site. This includes information about running Domain Name Services (DNS), types and names of domains on your network, and making a list of protocols used that need to pass through your security gateway.

**To collect your TCP/IP address information**

1 Do you currently run DNS on your network?

_____ Yes _____ No

2 What type of domain structure is in use at your site?

_____ Single domain _____ Multiple domains

_____ Subdomains

3 What type of name service do you provide?

_____ Primary name services _____ Secondary name services

_____ Internal/private

4 Do you have an internal name server?

_____ Yes _____ No

5 Do you have someone at your site who is knowledgeable about, and comfortable working with, DNS and how to configure it properly?

_____ Yes _____ No

6 If yes, who?

_____

7 Check the address types being used at your site.

_____ Registered IP address _____ Private IP address (RFC 1918)

_____ Unregistered IP address

Your connection to the Internet must have at least one public network address. You should use private, RFC 1918-compliant addresses internally or publicly registered IP addresses.

8 List the address ranges you currently use in your network.

_____

_____

9 List the protocols you use in your network.

_____

_____

10 Will you be using network news services (NNTP)?

_____ Yes _____ No

11 If yes, and you have your own internal NNTP server, record its IP address and the address of the server that will be supplying you with news feeds.

_____ Internal server: _____

_____ External news server: _____

---

**Note:** Only IP can be directly handled by the security gateway. Other protocols such as IPX cannot be serviced or passed through the security gateway.

---

# Defining your allowed TCP/IP services

Use the following tables to define all the allowed TCP/IP services in your network.

**To define your allowed TCP/IP services**

1 Use Table A-2 and check the access type (if any) you will allow for the following services.

**Table A-2** Allowed TCP/IP access type

| Access group | Telnet | SMTP | HTTPS | CIFS | HTTP | NNTP | RealAudio | RTSP | PING | Other |
|---|---|---|---|---|---|---|---|---|---|---|
| All users | | | | | | | | | | |
| All internal users | | | | | | | | | | |
| Selected group | | | | | | | | | | |
| No access | | | | | | | | | | |

2 Use Table A-3 to list your TCP/IP services.

**Table A-3** TCP/IP services

| | Group | Authentication | Access times |
|---|---|---|---|
| **FTP** | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| **Telnet** | | | |
| | | | |
| | | | |
| | | | |
| **HTTP** | | | |
| | | | |
| | | | |

**Table A-3** TCP/IP services (Continued)

| | Group | Authentication | Access times |
|---|---|---|---|
| | | | |
| **Other** | | | |
| | | | |
| | | | |
| | | | |

**Note:** Over time, you will likely refine these permissions. You should make periodic updates to this list.

3 Do you need transparent inbound access from the Internet (VPN)?

_____ Yes _____ No

## Collecting email information for security gateway notifications

You need to know information about email notifications. Use this section to collect data such as type of mail server, mail server IP address, mail transport protocol.

**To collect email information for security gateway notifications**

1 Record the name and IP address of your mail server.

Name: _____

Address:_____

2 Select the transport protocol being used for email.

_____ Third-party provided _____ POP3 mail

_____ SMTP mail

3 Does your Internet Service Provider provide a Mail Relay host?

_____ Yes _____ No

4 If yes, list its name and IP address.

_____ Mail relay host: _____

_____ Address: _____

5 List any mail programs you use internal to your network (for example, Microsoft Outlook):

_____

## Defining your Web services

Use the following section to define information about your Web services.

**To define your Web services**

1 Will you be using a Web server?

_____ Yes _____ No

2 If yes, select the location of the Web server.

_____ Internal to the security gateway

_____ External to the security gateway

3 Record the Web server name and IP address.

Name:_____ Address:_____

4 Will you be using an external caching/proxy server? If Yes, record the server name and IP address.

_____ Yes _____ No

Proxy server name:_____ Address:_____

5 Do you plan to use the content filtering service for security gateway?

_____ Yes _____ No

6 Do you plan to restrict access to any specific URLs?

_____ Yes _____ No

7 If yes, list the URLs to be restricted.

_____

_____

8 Use Table A-4 to list the names of any special services you wish to pass through the security gateway.

**Table A-4** Special services names

| Service name | Service port # | Service type (UDP/TCP) | Server name |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Access lists

List those entities and users to which you plan to write rules to allow access through the security gateway.

Use Table A-5 to list all entity identifications allowed.

**Table A-5** Entity identification

| IP address/DNS name | Entity type | Internal/external |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

**Table A-5** Entity identification (Continued)

| IP address/DNS name | Entity type | Internal/external |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

Use Table A-6 to list all user identities allowed.

**Table A-6** User identification

| User name | Account name | Group name |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## Defining your network architecture

In the following section, list all of the entities that comprise your network. Show all routers and computers systems that will be directly affected by, or connected to, the security gateway and its directly connected networks. Label each network component with its IP address and network mask.

Use Table A-7 to create a list of all internal servers. Your internal network consists of at least the security gateway host and a router.

**Table A-7** Internal network servers

| | DNS name services | Mail server | Web server | Other server |
|---|---|---|---|---|
| **Service** | | | | |
| **Host name** | | | | |
| **IP address** | | | | |
| **Subnet mask** | | | | |

Use Table A-8 to list your security gateway host system addresses.

**Table A-8** Security gateway host internal and external IP addresses

| Series host | Internal/external IP addresses |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Use Table A-9 to list your router IP addresses.

**Table A-9** Router IP addresses

| Router | IP addresses |
|---|---|
| | |
| | |
| | |
| | |
| | |

Your external network can also include external servers, such as an external Web server. Use Table A-10 to list all external network servers.

**Table A-10** External network servers

| | DNS name services | Mail server | Web server | Other server |
|---|---|---|---|---|
| **Service** | | | | |
| **Host name** | | | | |
| **IP address** | | | | |
| **Subnet mask** | | | | |

Appendix B

# Licensing

This appendix includes the following topics:


- Getting started with your 30-day grace period
- Easy steps for successful license implementation
- Understanding node count
- Using the Symantec License Request & Maintenance Web site
- Explanation of Symantec Enterprise Firewall licensing and maintenance
- About Symantec licenses


## Getting started with your 30-day grace period

To give you time to organize getting your license file, all the software included with your security gateway is enabled for a 30-day grace period. Features that require content updates, such as content filtering, require a license before you get new content.

Once you load and enable your license file, your 30-day grace period is no longer valid.

## Easy steps for successful license implementation

The following five easy steps provide for a successful license implementation:

- Gather your Serial Number Certificates
- Sort your serial numbers for each security gateway

- Collect product and contact information
- Plan for your license file
- Obtain your license file

## Gather your Serial Number Certificates

The first step in the process is to gather all your Serial Number Certificates. Symantec provides evidence of your purchase by means of a Serial Number Certificate. Check with your sales representative on how your certificates will be sent. Each Serial Number Certificate may contain several unique serial numbers, one for each license or service ordered.

## Sort your serial numbers for each security gateway

Serial numbers on Serial Number Certificates correspond to a particular order that you have placed, and may not apply to a particular security gateway. If you have placed orders for other Symantec products, you may find that the license serial numbers appear intermingled on the same Serial Number Certificate.

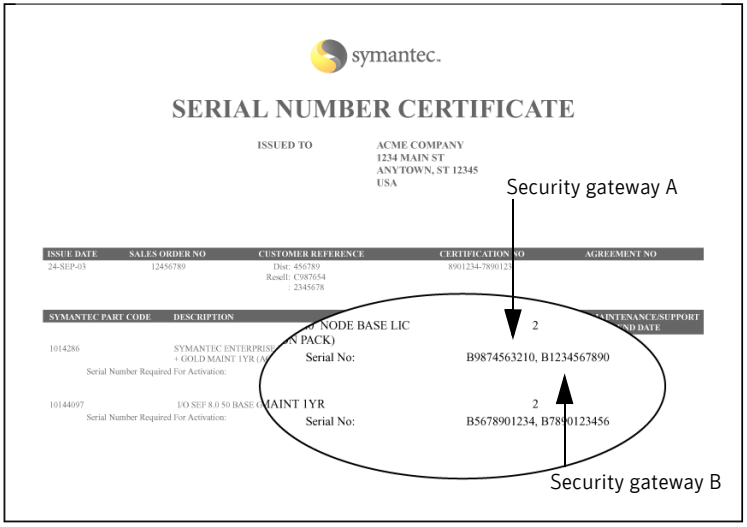
For example, if you ordered one security gateway, you won't have to worry about separating out numbers. If you ordered more than one security gateway, your serial numbers will be combined in the Serial Number Certificates and must be separated out. See Figure B-1, "Sample Serial Number Certificate," on page 83.

This appendix, provides a License File Organization Worksheet to ensure that you clearly identify which license serial numbers are used for each security gateway prior to generating for your license file. Make a copy of this worksheet for each security gateway you ordered, and complete each worksheet prior to obtaining your license file. See "License File Organization Worksheet" on page 89.

Figure B-1 shows serial numbers for features ordered for two different security gateways on the same certificate. It is highly recommended that you fill out a worksheet for each security gateway and separate these numbers.

See Table B-3, "License File Organization Worksheet," on page 89.

**Figure B-1** Sample Serial Number Certificate




## Collect product and contact information

You need the following information when completing the License File Organization Worksheet:

- The Symantec System ID.

  **Note:** The Symantec System ID is not the Host ID.

- The email address of the person to whom your license file for this security gateway should be sent.
- Names, phone and FAX numbers, and email addresses of two technical contacts.
- Full company name.

The Symantec System ID is an ID number that identifies your security gateway to the licensing system, which you can find through the products GUI, in the System folder > System Information tab.

**Warning:** The Symantec System ID is case sensitive.

Technical contact information (names, phone and FAX numbers) is required as only these two people can contact Symantec for technical support.

You must register for technical support and software update (maintenance) services at the same time that you request your license file.

Complete the License File Organization worksheet recording the serial numbers and the number of nodes licensed for each software component.

## Plan for your license file

When your license file is emailed to you, the only identifying information you receive is in the subject line of the email. The subject line contains one of the serial numbers included inside the license file. You must check your records and verify to which security gateway the license email applies and rename the file accordingly. You should create a distinguishable naming convention to easily identify the licenses when you go to upload this license file to the individual security gateways.

Your license file is attached to your email in a .zip file. Open this file using a decompression utility, such as WinZip or WinRAR.

The .slf file contained within the .zip file is the actual license file that you must load into your product to make it function.

Do not attempt to edit the .slf file in a text editor such as Notepad, Wordpad, or vi, as this will corrupt your license file and prevent your product from working properly.

If you need additional support to contact the Customer Service team for your region, on the Internet go to:

http://www.symantec.com/licensing/els/help/en/help.html

You must upload your license file to the security gateway before the 30-day grace period expires.

## Obtain your license file

To obtain your license file, on the Internet go to https://licensing.symantec.com and generate for your license.

For detailed instructions about licenses and the full procedure for obtaining your license see Appendix B of the *Symantec Enterprise Firewall Installation Guide*.

# Understanding node count

Understanding what a node is and how the security gateway enforces node licensing is important. A node is defined as any device that has a single IP address, such as: a computer, server, print server, terminal server, network photocopier, Symantec Client VPN, and so on. In the case where a protected node or any of these devices has more than one IP address, each one of the IP addresses counts as an additional node.

---

**Note:** You should configure a lease time on internal DHCP servers that is no less than 8 days with an address pool that does not exceed the total security gateway license count, taking into consideration nodes that have statically assigned IP addresses that are also protected by the security gateway.

---

When a protected node behind the security gateway acts as both a server and a client this counts as one node.

Symantec Client VPN sessions are counted based on active concurrent Client-to-Gateway VPN sessions.

In situations where a node is multi-homed, in other words, devices with more than one IP address, a license is required for each additional IP address assigned to the device.

The security gateway incrementally counts licenses based on the following:

- A single IP address (for example: a desktop/client machine with a single IP address) that initiates a connection or multiple connections through the security gateway counts as one license count.
- A connection or multiple connections to one protected server by way of a network interface marked as external (for example: a Web server with one IP address) behind the security gateway counts as one license count.
- A connection or multiple connections initiated from one IP address (acting as a client) in addition to a connection or multiple connections destined for the same IP address (acting as a server). See Figure B-2, “One IP address: one license,” on page 87.
- A Client-to-Gateway VPN session, independent of which direction traffic flow is initiated, counts as one connection.
  See Figure B-3, “Client-to-Gateway (five licenses),” on page 87.

Table B-1 shows the relationship between IP addresses and node count.

**Table B-1** Protected nodes behind a security gateway

| Device | Purpose | No. of IP addresses | Nodes/ license count |
|---|---|---|---|
| Desktop computer | Client | 1 | 1 |
| Web server | Server | 4 | 4 |
| Web server (or any device) | Server and client | 1 | 1 |

Table B-2 shows the relationship between Symantec Client VPNs and node count.

**Table B-2** Client-to-Gateway tunnels

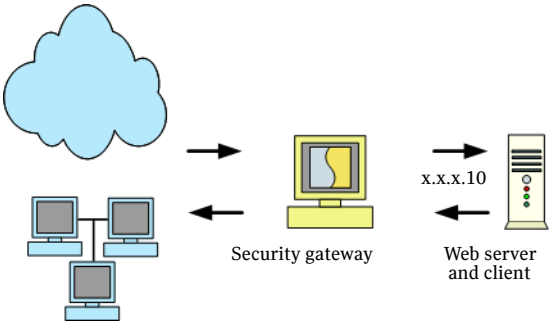
| Purpose | No. of IP addresses | Concurrent active sessions | Session/ license count |
|---|---|---|---|
| Symantec Client VPNs | 20 | 10 | 10 |

## Example scenario of when one IP address acts as client and server

Any node protected by the security gateway requires a license. If that node only acts as a client, it is counted once. If that node acts as both a client and a server it is counted once.

Figure B-2 shows one Web server acting as both a server and as a client. The security gateway counts this as only one license.

**Figure B-2** One IP address: one license

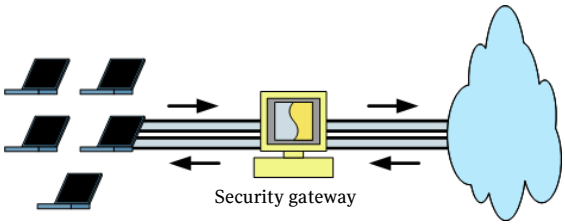



## How licenses are counted for Client-to-Gateway VPN

Licenses for Client-to-Gateway VPN sessions are available and incrementally counted by the number of concurrent remote sessions and are independent of which direction traffic flow is initiated.

Figure B-3 shows five remote Symantec Client VPN sessions. The security gateway counts this as five Client-to-Gateway licenses.

**Figure B-3** Client-to-Gateway (five licenses)




Once you understand this process you are ready to fill out the License File Organization Worksheet. See Table B-3, “License File Organization Worksheet,” on page 89.

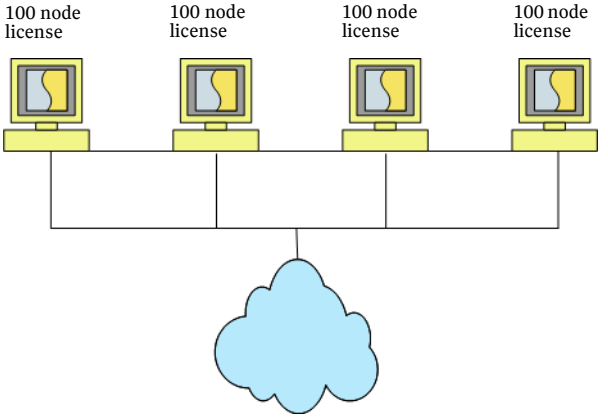
## Understanding nodes within clusters

A cluster is composed of multiple security gateways that are grouped together and configured to work as a single entity. A cluster ensures continued connectivity (high availability) and leverages processing power (load balancing) in the event that one or more security gateways within the cluster fails. Each

node in the cluster is required to have a license count as if it were the only security gateway protecting the network.

For example, if you need to protect a 100-node network, then each security gateway in the cluster must have at least a 100-node license size.

**Figure B-4** License size for a cluster



You must fill out the worksheet in Table B-3 before you apply for your license file.

**Table B-3** License File Organization Worksheet

| | | | |
|---|---|---|---|
| **I. Certificate number** | | | |
| **II. Symantec System ID number** | | | |
| **III. Base Firewall (Includes unlimited Gateway-to-Gateway VPN and one Client-to Gateway VPN)** | | | |
| Part codes | Description | License nodes | Serial number |
| | Base license | | |
| N/A | Base maintenance | | |
| **IV. Firewall (Additive nodes)** | | | |
| Part codes | Description | License nodes | Serial number |
| | | | |
| | | | |
| | | | |
| **V. Virtual Private Network (Additive Client-to Gateway sessions)** | | | |
| Part codes | Description | License nodes | Serial number |
| | | | |
| | | | |
| | | | |
| **VI. High Availability/Load Balancing (One license per security gateway)** | | | |
| Part codes | Description | License nodes | Serial number |
| 10142194 | Symantec Enterprise Firewall 8.0, HA/LB function add-on license plus Gold Maintenance up to 1 year | N/A | |

**Table B-3** License File Organization Worksheet (Continued)

| **VII. Content filtering (Function add-on)** | | | |
|---|---|---|---|
| Part codes | Description (license or maintenance) | License nodes | Serial number |
| | Symantec Enterprise Firewall 8.0, CF function add-on license plus Gold Maintenance up to 1 year | | |
| | | | |
| | | | |

# Using the Symantec License Request & Maintenance Web site

The Symantec Enterprise Firewall software is shipped with a license that lets the software operate for a 30-day grace period. This license begins when you install the product. You must obtain a license file within the 30-day grace period to continue using the product.

## Getting your license files

To activate your license you must have the base Software Serial Number Certificate. This is the first level of information you are prompted for from the licensing Web site.

**Note:** The license file you generate applies to one security gateway only.

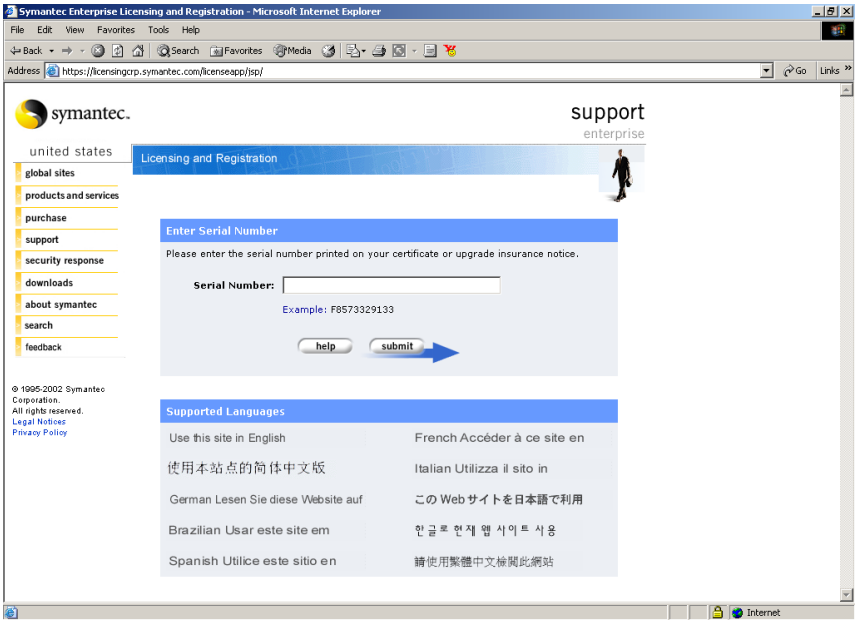
If you are also enabling other features for this security gateway, have those serial numbers ready as well. When you apply for your license file, be aware that all the serial numbers you input apply to a specific security gateway. Do not mix serial numbers that apply to features you want to enable on other security gateways.

### Before you get your license file

Before you go to get your license, you should have filled out a License Organization Worksheet for each security gateway that you have ordered. Once you have completed that form, you are ready to proceed.

### To get your license file

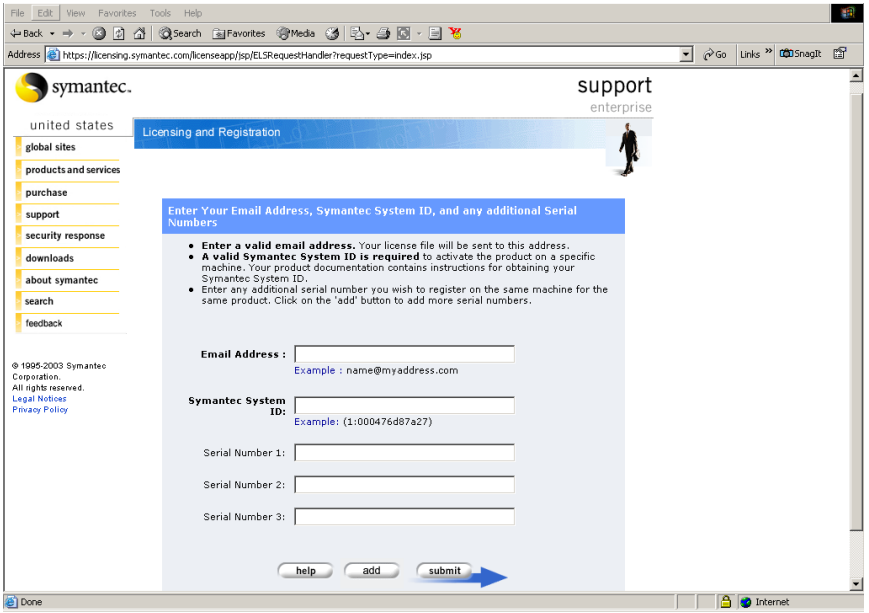
1 Browse to https://licensing.symantec.com.




2 In the Licensing and Registration page, under Supported Languages, select your language.

3 Under Enter Serial Number, in the Serial Number text box, type your base software serial number.
This is the serial number found on the base Software Serial Number Certificate for the base firewall license.

4 Click **submit**.


File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://licensing.symantec.com/licenseapp/jsp/ELSRequestHandler?requestType=index.jsp
Go Links SnagIt
symantec.
support
enterprise
united states
global sites
products and services
purchase
support
security response
downloads
about symantec
search
feedback
Licensing and Registration
Enter Your Email Address, Symantec System ID, and any additional Serial Numbers
Enter a valid email address. Your license file will be sent to this address.
A valid Symantec System ID is required to activate the product on a specific machine. Your product documentation contains instructions for obtaining your Symantec System ID.
Enter any additional serial number you wish to register on the same machine for the same product. Click on the 'add' button to add more serial numbers.
Email Address :
Example : name@myaddress.com
Symantec System ID:
Example: (1:000476d87a27)
Serial Number 1:
Serial Number 2:
Serial Number 3:
help
add
submit
© 1995-2003 Symantec Corporation.
All rights reserved.
Legal Notices
Privacy Policy
Done
Internet

5 Under Enter Your Email Address, Symantec System ID, and any additional Serial Numbers, do the following:

- In the Email Address text box, type the email address of the person managing the license files.
  The license file is mailed to this address.
- In the Symantec System ID text box, type your security gateway Symantec System ID.
  A valid Symantec System ID is required to activate the product on a specific machine.You can find the Symantec System ID using the SGMI by accessing the System folder > System Information tab.

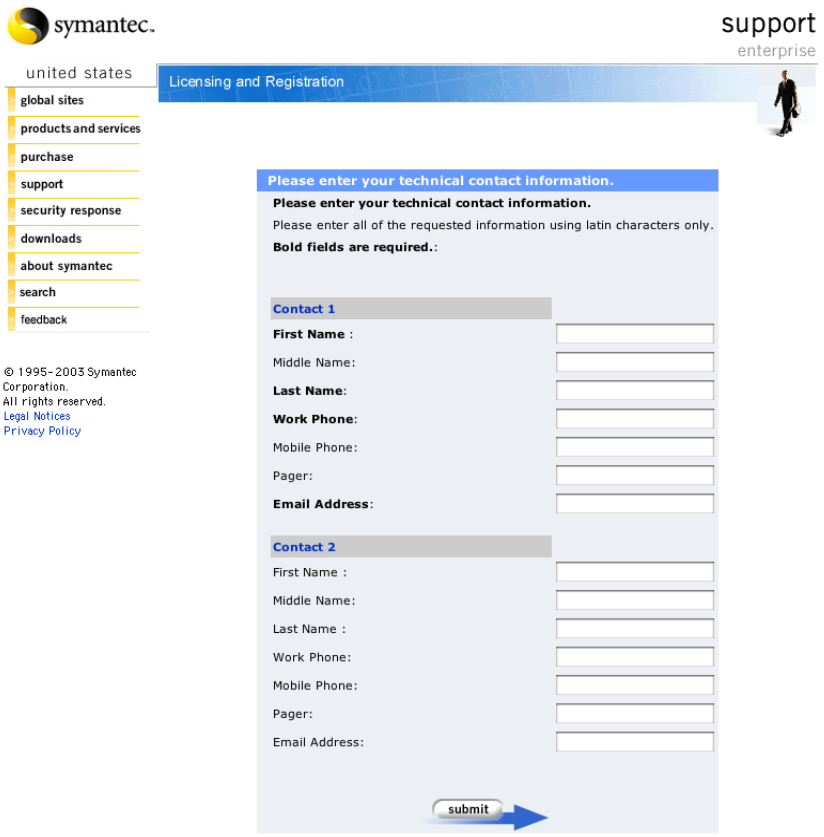
**Warning:** You must include the parentheses when you type they Symantec System ID; for example, (5:3CB7-83C7).

- In the Serial Number text boxes, type any additional security gateway serial numbers, which you can find on the Serial Number Certificates. Include your maintenance serial number for this security gateway. It does not matter in which order the numbers are typed.

**Warning:** These are serial numbers that are associated with licenses purchased for this security gateway only.

6 If you have more than three serial numbers to enter, click **add**.
Clicking add inserts new fields above the ones you have already filled in. You can now input any additional serial numbers you may have. You can click add as many times as you need to add all of your serial numbers.

7 When you are finished, click **submit.**

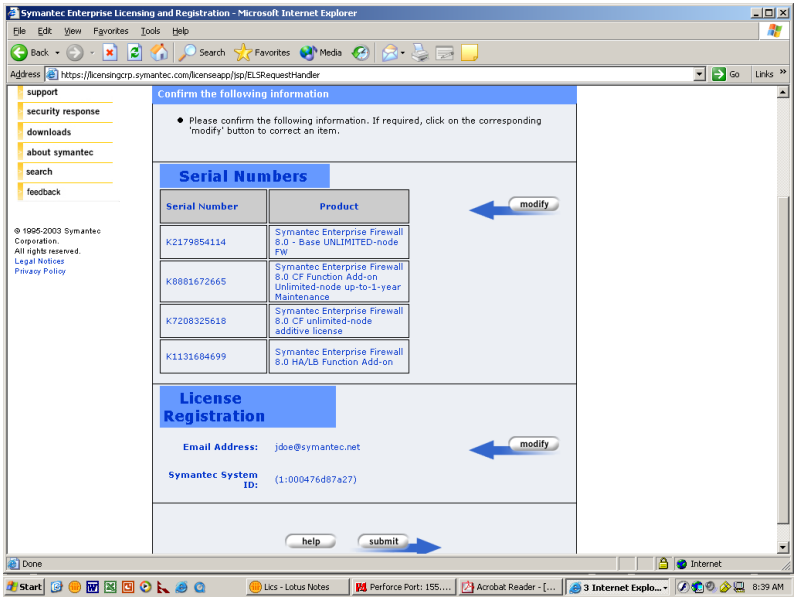



8 On the technical contact information page, under Contact 1, do the following:

- In the First Name text box, type the first name of your technical contact.
- In the Last Name text box, type the last name of your technical contact.
- In the Work Phone text box, type the phone number of your technical contact.
- In the Email Address text box, type the email address of the technical contact.

If you have an additional contact, fill in the information under Contact 2.

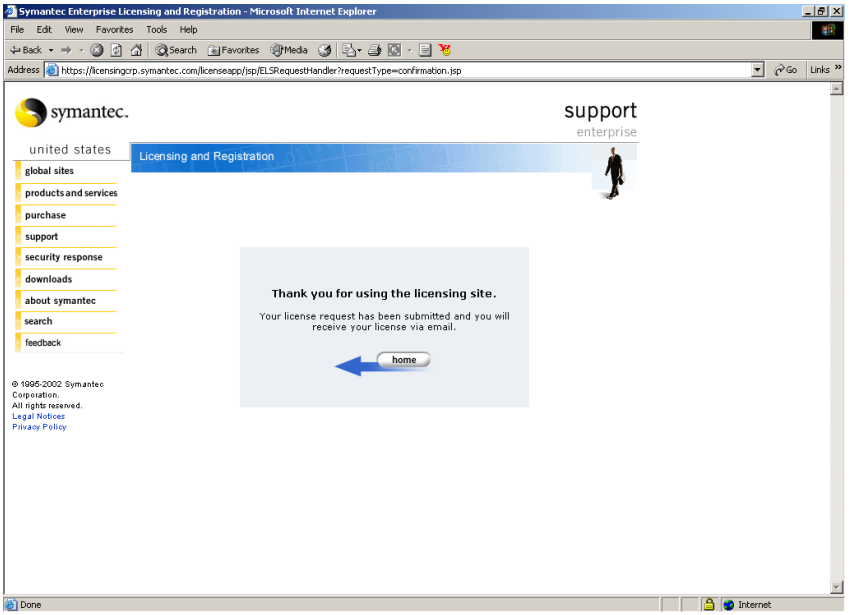
9 Click **submit**.




10 Under Confirm the following information, do the following:

- Under Serial Numbers, confirm the serial numbers and products you have registered.
- Under License Registration, confirm your email address and Symantec System ID.
- Under Support Registration, confirm your maintenance serial number, and the two support contacts for your product.
- Under Security Gateway Registration, confirm your product serial number, name, company name, company address, work phone, and email address for a company contact responsible for this product.

11 Click **submit**.




The person you specified receives an email from Symantec with an attached license file, which he or she can use to enable all the product features registered. The subject line of that email contains a serial number for one of the licensed products contained within the order. Copy your license files to a known directory, rename them, and move them to a system you use to manage your security gateway.

---

**Note:** Once you receive, rename, and store your license files, keep a backup of these files in a safe place.

---

If you purchase additional licenses for this security gateway in the future, you should follow these same steps for the new licenses and associated serial numbers. Note that old serial numbers are not reentered. Multiple license files are applied to a single security gateway and licenses are additive.

## Uploading your license files

If you have already completed your initial setup and configuration, have been using your 30-day grace period, and are now ready to install your license files, you can install your licenses by going to the SGMI System folder > Features tab > Installed Licenses window.

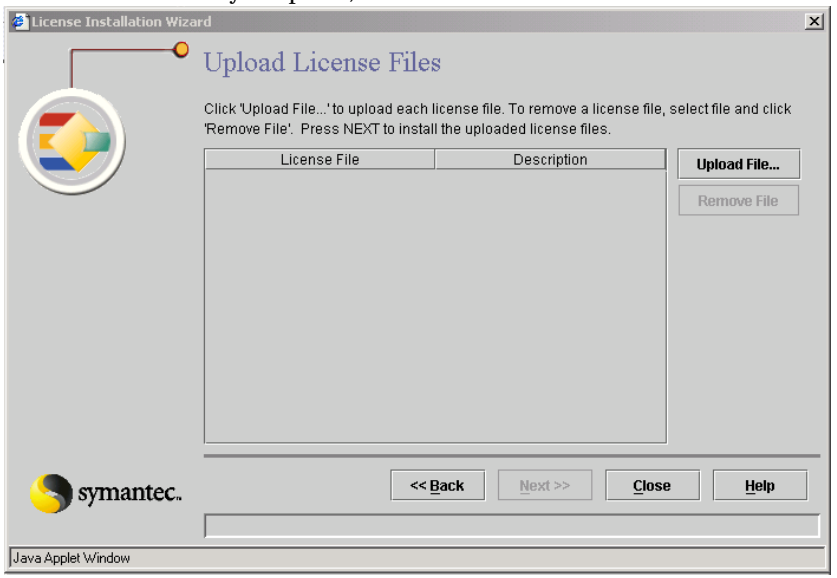
### To upload your license files

1 In the left pane of the SGMI, click **System**.

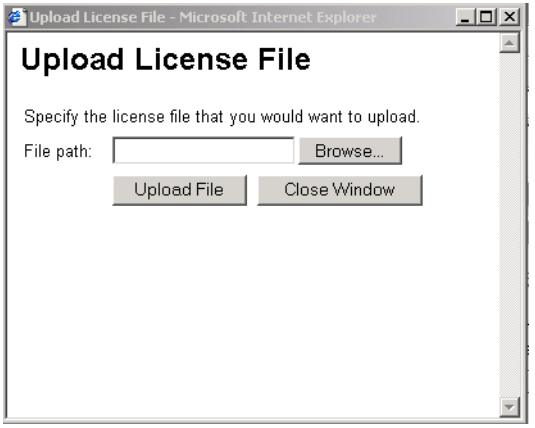
2 In the right pane, on the Feature tab, click **Installed Licenses**.

3 Click **Install**.

4 On the Welcome to the License Installation Wizard panel, if you have the license files ready to upload, click **Next**.




5 On the Upload License Files panel, click **Upload File**.




6 In the Upload License File panel, browse to where you have saved your license files, and then do the following:

- Select a license file, and then click **Upload File**.
- Repeat steps 5 and 6 for all license files.
- When finished, click **Close Window**.

7 On the License Error Check panel, read the message, and then do the following:

- If there were no errors found, click **Next**.
- If there were errors found, you must click **Close**. Call Symantec Technical Support for assistance.

8 On the Confirm License Installation panel, verify that all the features and node limits you want are uploaded, and to install them on the security gateway, click **Next**.
Otherwise, click **Back** and install any missing license files.

9 On the License Installation Complete panel, click **Close**.

## Removing license files

If you must remove a license file, contact Symantec Technical Support.

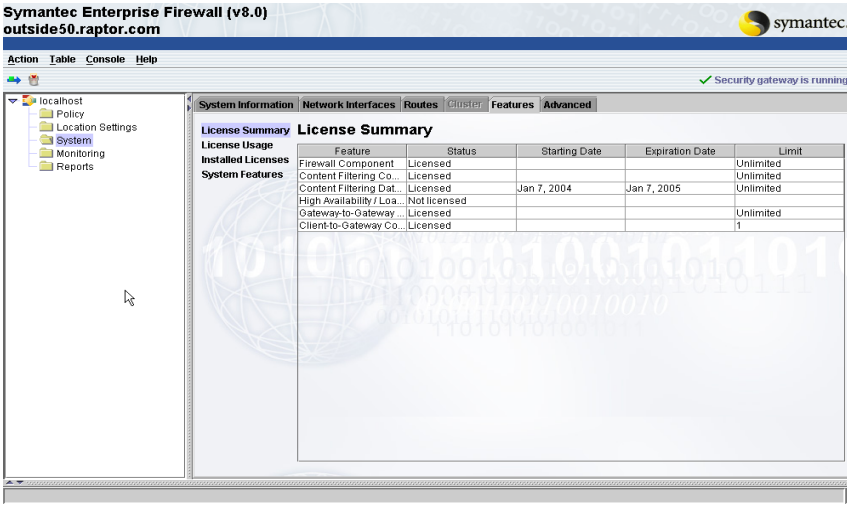
## Viewing license enabled features

The security gateway software is covered by the Symantec license included with the license serial number. You can view your enabled features using the SGMI.

### To view licensed and enabled features

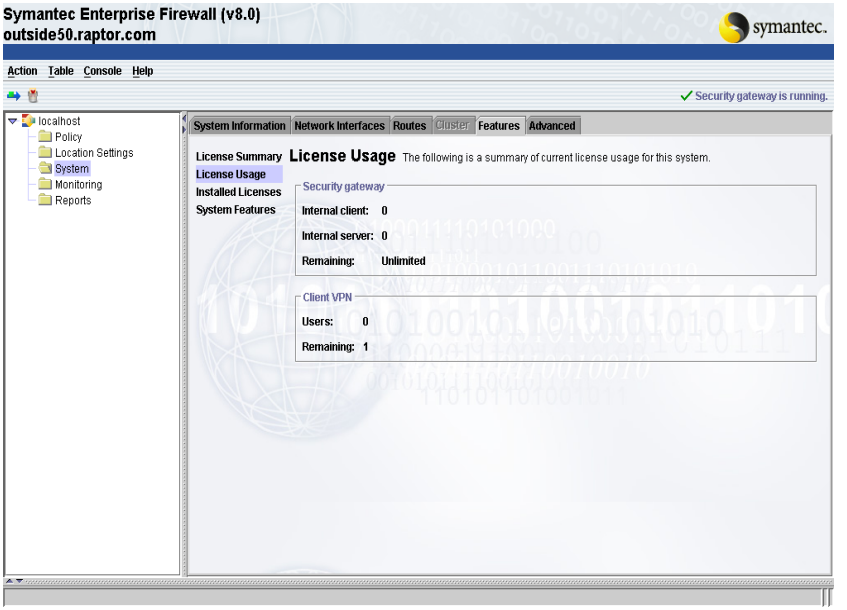
1 In the left pane, click **System**.

2 In the right pane, on the Features tab, click **License Summary**.




The license Feature, Status, Starting Date, Expiration Date, and Limit (node count) are displayed in the right pane.

3 To view your actual usage, click **License Usage**.



# Explanation of Symantec Enterprise Firewall licensing and maintenance

Symantec Enterprise Firewall usage is controlled by a licensing scheme. A license is required for each function that you want to use. Without it, the function is not enabled.

## Session licensing for Symantec Client VPN

Symantec Client VPN software is licensed with a security gateway. The Symantec Client VPN software version must match the associated security gateway software version. Client-to-Gateway VPN is licensed by the number of concurrent VPN sessions. The security gateway comes with a license for one Client-to-Gateway VPN session. You can purchase additional licenses for concurrent VPN sessions. For example, you may have 100 users who need VPN access as part of their normal work habits, but at any time, only 10 users are ever connected by way of the VPN. In this situation, you only need a license for 10 concurrent VPN sessions. The security gateway counts the number of concurrent Client-to-Gateway VPN sessions and stops creating new sessions when the limit is reached. You are licensed to load the client software on as many nodes as you like, but these clients are licensed for use only with the accompanying security gateway.

## High Availability and Load Balancing (HA/LB)

HA/LB is licensed on a per-security gateway basis. It is either enabled or disabled. It is not licensed by cluster. For a two-node cluster, you need two High Availability load balancing licenses, one for each cluster node.

## Obtaining a license file

When you purchase a license, Symantec provides you with a software Serial Number Certificate.

## Basic license types

Each security gateway needs a base license, which includes a license for firewall, unlimited Gateway-to-Gateway VPN, and one concurrent Client-to-Gateway VPN user.

## Function add-ons

Function add-ons are available to add content filtering and HA/LB. Function add-ons for content filtering must match the base node firewall license. HA/LB is licensed on a per-security gateway basis.

## Additive licenses

Additive licenses are available to increase the number of nodes protected by the security gateway, increase the number of nodes for content filtering (firewall and content filtering must both be the same size), and to increase the Symantec Client VPN sessions.

Additive licenses include additive firewall, content filtering node licenses, and additive Symantec Client VPN licenses. Session licenses relate to VPN and node licenses relate to the firewall and content filtering features.

Additive node licenses are cumulative. For example, you can buy a 25-node additive license for firewall and add it to the base 25-node base firewall license to get a resultant license of 50 nodes. You could then purchase a 100-node firewall additive node license and add it to the previous 50-node license to get a resultant 150 node license.

---

**Note:** You must license firewall and content filtering for the exact same number of nodes. This means that a you cannot have a 75-node license for firewall and a 50-node content filtering. Each feature would have to have a 75-node license.

---

Additive licenses are available for Client-to-Gateway VPN. Client-to-Gateway VPN session licenses are independent of node licenses and the two can have different values.

## License certificates

You must order the security gateway with a base security gateway license. The Serial Number Certificate is sent to you and contains a software serial number, which, when combined with the security gateway Symantec System ID, is used to generate a license file. This license file normally enables a firewall, unlimited Gateway-to-Gateway VPN, and one concurrent Client-to-Gateway VPN user.

Separately orderable function add-ons and additive licenses are enabled by additional software serial numbers that come on an additional Serial Number Certificate. Each certificate has space for one or more software serial numbers. When you order one or more feature add-on and/or additive license at the same time, one or more Serial Number Certificates are sent to you.

### 30-day grace period

The security gateway runs for 30 days without a license file. This 30-day grace period is for unlimited nodes for all features (firewall, Gateway-to-Gateway VPN, and content filtering) and unlimited Client-to-Gateway VPN users. However, a license file is necessary to enable the software on the security gateway to run after this 30-day grace period has expired. You obtain a license file by accessing the Symantec licensing Web site. The 30-day grace period does not enable LiveUpdate. However, initial sample content is shipped with the product for content filtering.

## Content updates

Content filtering is updated with new URL list updates. These updates are provided as a subscription with your maintenance agreement. When you purchase a function add-on, it enables a subscription for that feature for the duration of your current maintenance agreement. All content subscription updates expire on the same day as the maintenance contract for the security gateway. Maintenance renewals include content subscription updates for the length of the renewal contract.

## Maintenance contracts

Except for the first year, separate maintenance contracts are available for renewal for the security gateway functions.

### Symantec Enterprise Firewall

All base licenses include a Gold Maintenance contract for the first year. This Gold Maintenance contract starts from the day the security gateway is purchased and lasts for one year. The Gold Maintenance contracts include:

- Business-hour telephone support.
- Upgrade insurance, which includes an entitlement to any new versions of the security gateway software released by Symantec during the term of the contract.
- Content updates for content filtering (if these associated function licenses have been purchased).

Function add-ons and additive licenses include maintenance for up to one year for the function or increased number of nodes or users if the base security gateway is currently covered by a maintenance agreement. This maintenance is tied to the basic security gateway contract and expires on the same date.

Gold Maintenance is included for up to one year in the price of the additive user licenses. Platinum is an uplift to the Gold maintenance. The contract co-terminates with the base security gateway contract. You must purchase either Gold or Platinum renewals at the same time and for the same duration as the security gateway renewal.

Platinum support is available as an uplift to Gold maintenance. The contract co-terminates with the base security gateway contract. You must purchase Gold and Platinum renewals at the same time and for the same duration as the security gateway renewal.

### Maintenance renewals

One-year maintenance renewal contracts are available for all features and HA/LB maintenance renewal contracts are separate, but are tied to the expiration of the basic security gateway contract.

### Platinum support uplift

You may need continuous availability of telephone support (24 x 7). This is provided for by a Platinum support uplifts to the Gold contract. For subsequent years, Platinum support uplift contracts are also available.

## About Symantec licenses

The security gateway software is covered by the Symantec Software License Agreement. The license agreement grants the licensee the right to use the software on the associated security gateway.

### SYMANTEC SOFTWARE LICENSE AGREEMENT SYMANTEC ENTERPRISE FIREWALL

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND

CONDITIONS, CLICK THE "I DO NOT AGREE," OR "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

## 1. License:

Except for the software excluded below, the software and documentation that accompanies this license (collectively the ""Software"") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Software, Your rights and obligations with respect to the use of this Software are as follows.

## You may:

A. use that number of licenses of the Software as have been licensed to you by Symantec under a License Module. Your License Module shall constitute proof of your right to use such number of licenses. If no License Module accompanies, precedes, or follows this license agreement, you may use one license of the Software;
B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
C. use the Software for no more than the number of users set forth in the applicable License Module for your own internal business purposes
D. use the Software in accordance with any written agreement between You and Symantec; and
E. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees in writing to the terms of this license.

## You may not:

A. copy the printed documentation that accompanies the Software;
B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
D. continue to use a previously issued license key if you have received a new license key for such license, such as with a disk replacement set or an upgraded version of the Software, or in any other instance
E. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
F. use a later version of the Software than is provided herewith unless you You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;
G. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module; nor
H. use the Software in any manner not authorized by this license.

## 2. Content Updates:

Certain Software utilize content which that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions;

content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates which that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit Licensee the licensee to obtain and use Content Updates.

## 3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

## 4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
IN NO CASE SHALL SYMANTEC'S SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you or not You accept the Software.

## 5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are ""Commercial Items"," as that term is defined in 48 C.F.R. section 2.101, consisting of ""Commercial Computer Software"" and ""Commercial Computer Software Documentation"," as such

terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

## 6. Export Regulation:

Export, or re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries. Export or re-export of the Software to any entity not authorized by, or that is specified on the Denied Parties List and other lists promulgated by various agencies of the United States Federal Government is strictly prohibited.

## 7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module which that accompanies this license or by a written document which that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Authorized Service Center, Postbus 1029, 3600 BA Maarssen, The NetherlandsSymantec Customer Service Center, PO BOX 5689, Dublin 15,Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

## 8. Excluded Software

The excluded software consists of the open source code software known as Linux. All excluded software is licenses under the GNU General Public License, Version 2, June 1991, a copy of which is included with the user documentation where applicable. The license entitles You to receive a copy of the source code for Linux only upon request at a nominal charge. If You are interested in obtaining a copy of such source code, please contact Symantec Customer Service at one of the above addresses for further information.

Appendix C

# Troubleshooting

This appendix includes the following topics:


- Accessing troubleshooting information


## Accessing troubleshooting information

You can find up-to-date troubleshooting information for the Symantec Enterprise Firewall (and all Symantec products) on the Symantec Web site, www.symantec.com.

Use the following procedure to access troubleshooting information from the Symantec Knowledge Base.

**To access Symantec Enterprise Firewall troubleshooting information**

1. Go to www.symantec.com.
2. On the top of the home page, click **support.**
3. Under Product Support > enterprise, click **Continue.**
4. On the Support enterprise page, under Technical Support, click **knowledge base**.
5. Under select a knowledge base, scroll down and click **Symantec Enterprise Firewall**.
6. Click on your specific product name and version.

7 On the knowledge base page for Symantec Enterprise Firewall, do any of the following:

- On the Hot Topics tab, click any of the items in the list to view a detailed list of knowledge base articles on that topic.
- On the Search tab, in the text box, type a string containing your question. Use the drop-down list to determine how the search is performed, and then click **Search**.
- On the Browse tab, expand a heading to see knowledge base articles related to that topic.

# Index


## Numerics

30-day grace period 81, 91, 102

## A

access lists, checklists 77
advanced configurations 55
authentication method, checklist 70

## B

browser support 11, 13

## C

certificate, sample 83
configuration, System Setup Wizard 40, 48
content updates 102
CPU
    recommended (Microsoft Windows) 12
    recommended (Sun Solaris) 14

## D

datalink drivers
    HA/LB (Microsoft Windows) 16
    HA/LB (Sun Solaris) 17
DHCP, restrictions with Symantec Enterprise Firewall 23, 85
disabling, unauthorized services using Vulture (Microsoft Windows) 27
disk space
    recommended (Microsoft Windows) 13
    recommended (Sun Solaris) 14
DNSd, configuring (Microsoft Windows) 22
documentation, supplied 18
domestic encryption, selecting 26

## E

enabling external PING 47, 54
encryption type, selecting 26

## G

Gold Maintenance 102

## H

hardware requirements
    Microsoft Windows security gateway 12
    Sun Solaris security gateway 14
heartbeat interface 45, 47, 52, 54
high availability/load balancing 45, 52
host system interfaces, testing 24, 32

## I

installing
    RemoteLog (Microsoft Windows) 27
    RemoteLog (Solaris) 34
    security gateway (Microsoft Windows) 26
    security gateway (Solaris) 33
international encryption, selecting 26
IP addresses
    configuring (Microsoft Windows) 22
    configuring (Sun Solaris) 30
    verifying (Microsoft Windows) 23
    verifying (Sun Solaris) 31
IP addresses checklist 73

## J

Java Runtime Environment, see JRE
JRE
    supported version 11, 40
    supported versions 12

## L

license
    30-day grace period 81
    License File Organization Worksheet 89
    obtaining 38, 84
    serial number certificates 82
    types 100
license files

installation 44, 50
removing 96, 98
uploading 96
viewing 98
License Installation Wizard 44, 50
license serial number
obtaining 82
organizing 82
licensing and maintenance 100

## M

maintenance
contracts 102
Gold 102
renewals 103
memory (RAM)
recommended (Microsoft Windows) 13
recommended (Sun Solaris) 14
Microsoft Internet Explorer, supported version 11
Microsoft Windows
configuring DNSd 22
setting computer name 22
setting IP addresses 22
setting TCP/IP options 22
Microsoft Windows security gateway
hardware requirements 12

## N

Netscape, supported version 11
network configuration, testing 23
network connectivity
checking after installation 59
troubleshooting 62
network interface cards
supported 12, 15
unsupported 18
network settings
testing 23
network, architecture checklist 78
news service, checklist 76
NICs, adding, removing, or changing 62
node count, defining 85

## O

obtaining, license file 91
operating system
configuring (Microsoft Windows) 21
configuring (Sun Solaris) 29
supported platforms 12

## P

password, logon 40, 47
PING, external interface 47, 54
Platinum support 103
product component list 18
proxies, checklist 74

## R

RemoteLog
installing (Microsoft Windows) 27
installing (Solaris) 34
removing license file 96, 98
restore a previous configuration 40
routing tables, requirements 22

## S

security plan
checklist 65
worksheets 68
serial number certificate, sample 83
serial number certificates 101
setting up, security gateway 47
SGMI
browser address 41, 48
System Setup Wizard 40, 48
site hardware information, checklist 71
software requirements
Microsoft Windows security gateway 12
Sun Solaris security gateway 14
software serial number certificate 91
Symantec System ID
definition 84
where to enter it 93
why you need it 83
System Setup Wizard 40, 48

## T

TCP/IP
setting options (Microsoft Windows) 22
verifying settings (Microsoft Windows) 23
verifying settings (Sun Solaris) 31
TCP/IP checklist 72
testing
basic connectivity 59

network configuration 23
troubleshooting 107
failed installation 59
possible problems 59

## U

unauthorized services, Vulture 27
uninstalling
security gateway software (Microsoft Windows) 55
security gateway software (Sun Solaris) 56
upgrade limitations 39
upgrade, using System Setup Wizard 40
upgrading security gateway
(Microsoft Windows) 25
(Sun Solaris) 32
uploading license files 44, 50
user documentation 18

## V

verifying, installation 59
viewing license file 98
Vulture
disabling unauthorized services 27
setting activation frequency 27

## W

WEB service, checklist 76
wizards
License Installation Wizard 44, 50
System Setup Wizard 40, 48
worksheets, security planning 68